

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Akira YAEGASHI

Art Unit: N/A

Application No.: Not Yet Assigned

Filed: March 26, 2004

For: IMAGE TRANSMISSION SYSTEM, IMAGE
PICKUP APPARATUS, IMAGE PICKUP
APPARATUS UNIT, KEY GENERATING
APPARATUS, AND PROGRAM

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
Japan	P2003-101783	April 4, 2003

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: March 26, 2004

Respectfully submitted,

By  *ROBERT S. GRAUER*
Ret. No. 41,800

Ronald P. Kananen

Registration No.: 24,104

Rader, Fishman & Grauer PLLC
Suite 501
1233 20th Street, N.W.
Washington, D.C. 20036
Telephone: (202) 955-3750
Facsimile: (202) 955-3751
Customer No.: 23353

日 本 国 特 許 庁
JAPAN PATENT OFFICE

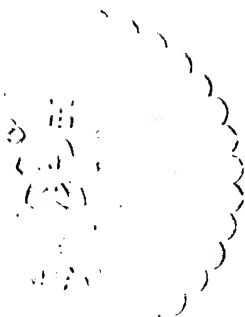
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 4 月 4 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 0 1 7 8 3
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 1 0 1 7 8 3]

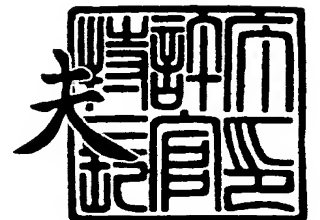
出 願 人 ソニー株式会社
Applicant(s):



2 0 0 4 年 2 月 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0390074707

【提出日】 平成15年 4月 4日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 H04L 9/00
G09C 1/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 八重樫 章

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100095957

【弁理士】

【氏名又は名称】 亀谷 美明

【電話番号】 03-5919-3808

【選任した代理人】

【識別番号】 100096389

【弁理士】

【氏名又は名称】 金本 哲男

【電話番号】 03-3226-6631

【選任した代理人】

【識別番号】 100101557

【弁理士】

【氏名又は名称】 萩原 康司

【電話番号】 03-3226-6631

【手数料の表示】

【予納台帳番号】 040224

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0012374

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像伝送システム、撮像装置、撮像装置ユニット、鍵生成装置、およびプログラム

【特許請求の範囲】

【請求項 1】 ネットワークを介して画像を送送する画像伝送システムであって、

各々が固有の識別番号を有し、撮像した画像を暗号化して前記ネットワークに伝送するための暗号化機能を有する 1 または 2 以上の撮像装置と、

前記画像を暗号化するための暗号化キーおよび前記暗号化された画像を復号化するための復号化キーを前記撮像装置ごとに生成する鍵生成装置と、

前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と、

前記リムーバブル記録媒体が接続され、前記復号化キーを用いて前記暗号化された画像を復号化する復号化機能を有し、前記ネットワークを介して前記撮像装置が伝送する画像を閲覧するための閲覧装置と、

前記閲覧装置からアクセス可能な前記撮像装置の認証を行う認証サーバと、を含むことを特徴とする、画像伝送システム。

【請求項 2】 ネットワークを介して画像を送送する画像伝送システムであって、

各々が固有の識別番号を有する 1 または 2 以上の撮像装置と、

前記撮像装置が撮像した画像を暗号化して前記ネットワークに伝送するとともに、前記暗号化された画像の復号化するための復号化キーを生成する鍵生成装置と、

前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と、

前記リムーバブル記録媒体が接続され、前記復号化キーを用いて前記暗号化された画像を復号化する復号化機能を有し、前記ネットワークを介して前記撮像装置が伝送する画像を閲覧するための閲覧装置と、

前記閲覧装置からアクセス可能な前記撮像装置の認証を行う認証サーバと、

を含むことを特徴とする、画像伝送システム。

【請求項 3】 ネットワークを介して画像を送送する画像伝送システムであって、

各々が固有の識別番号を有する 1 または 2 以上の撮像装置と、

前記撮像装置が撮像した画像を暗号化して前記ネットワークに伝送する伝送装置と、

前記画像を暗号化するための暗号化キーおよび前記暗号化された画像を復号化するための復号化キーを前記撮像装置ごとに生成する鍵生成装置と、

前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と、

前記リムーバブル記録媒体が接続され、前記復号化キーを用いて前記暗号化された画像を復号化する復号化機能を有し、前記ネットワークを介して前記撮像装置が伝送する画像を閲覧するための閲覧装置と、

前記閲覧装置からアクセス可能な前記撮像装置の認証を行う認証サーバと、を含むことを特徴とする、画像伝送システム。

【請求項 4】 ネットワークを介して画像を送送する画像伝送システムであって、

各々が固有の識別番号を有し、撮像した画像を暗号化して前記ネットワークに伝送するための暗号化機能を有する 1 または 2 以上の撮像装置と、

前記撮像装置が画像を暗号化するための暗号化キーおよび復号化キーを前記撮像装置ごとに生成する鍵生成装置と、

前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と、

前記リムーバブル記録媒体が接続され、前記復号化キーを用いて前記暗号化された画像を復号化する復号化機能を有し、前記ネットワークを介して前記撮像装置が伝送する画像を閲覧するための閲覧装置と、

を含むことを特徴とする、画像伝送システム。

【請求項 5】 ネットワークを介して画像を送送する画像伝送システムに用いられる撮像装置であって、

固有の識別番号を記録する記録部と、
撮像した画像を暗号化する暗号化部と、
前記暗号化された画像をネットワークに伝送する通信部と、
を備えたことを特徴とする、撮像装置。

【請求項 6】 前記通信部は、前記画像を暗号化するための暗号化キーを鍵生成装置から受信する受信部を含むことを特徴とする、請求項 5 に記載の撮像装置。

【請求項 7】 前記通信部は、USB ポートを含むことを特徴とする、請求項 5 に記載の撮像装置。

【請求項 8】 前記記録手段は、IP アドレスを記録することを特徴とする、請求項 5 に記載の撮像装置。

【請求項 9】 固有の識別番号を有し、撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する撮像装置と、
前記撮像装置が暗号化した画像を復号化するための復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と、
を含むことを特徴とする、撮像装置ユニット。

【請求項 10】 前記撮像装置は、前記画像を暗号化するための暗号化キーを鍵生成装置から受信することを特徴とする、請求項 9 に記載の撮像装置ユニット。

【請求項 11】 前記リムーバブル記録媒体は、前記画像を復号化するための復号化キーを鍵生成装置から受信することを特徴とする、請求項 9 に記載の撮像装置ユニット。

【請求項 12】 前記撮像装置は、USB カメラであることを特徴とする、請求項 9 に記載の撮像装置ユニット。

【請求項 13】 前記撮像装置は、IP カメラであることを特徴とする、請求項 9 に記載の撮像装置ユニット。

【請求項 14】 ネットワークを介して画像を伝送する際の暗号処理に用いられる暗号化キーおよび復号化キーを生成する鍵生成装置であって、
固有の識別番号を有し、撮像した画像を暗号化してネットワークに伝送するた

めの暗号化機能を有する撮像装置に対して、前記画像を暗号化するための暗号化キーを生成して送出するとともに、

前記暗号化された画像を復号化するための復号化キーを生成して、前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体に送出することを特徴とする、鍵生成装置。

【請求項 15】 前記撮像装置を前記ネットワークに中継する中継機能を有することを特徴とする、請求項 14 に記載の鍵生成装置。

【請求項 16】 前記撮像装置が撮像した画像を圧縮する圧縮機能を有することを特徴とする、請求項 14 に記載の鍵生成装置。

【請求項 17】 コンピュータを、請求項 14 に記載の鍵生成装置として機能させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は画像伝送システムおよびその関連技術にかかり、特に、家庭やオフィス内の監視を行うセキュリティサービスに利用可能な画像伝送システム、撮像装置、撮像装置ユニット、鍵生成装置、およびプログラムに関する。

【0002】

【従来の技術】

近年におけるネットワーク技術の発展にはめざましいものがあり、ネットワークを介して様々な情報のやりとりが可能な環境が整っている。このような中で、家庭やオフィス内にカメラを設置し、カメラからの映像や静止画などをネットワークを介して伝送することで、遠隔地から家庭やオフィス内の様子を監視する監視システムがある（例えば、特許文献 1 参照。）。このような監視システムは、家庭やオフィスの防犯のほか、留守中のペットを監視したり、遠隔地に住む一人暮らしの老人の様子を確認したりといった様々な利用法がある。

【0003】

【特許文献 1】

特開 2002-183860

【 0 0 0 4 】

【発明が解決しようとする課題】

上述のように、ネットワークを介して様々な情報のやりとりが可能な環境が整ってきたことにともない、ネットワークにおけるセキュリティ確保の問題が顕在化しつつある。すなわち、ネットワークを介して様々な情報を容易にやりとりできる反面、その情報は、悪意を持った第三者から盗聴されるという危険を常に抱えている。このような問題は、プライバシー保護の観点からも近年クローズアップされつつあり、その対策が急務である。

【 0 0 0 5 】

また、上述の監視システムでは、家庭やオフィスと監視会社とを専用線で結ぶことでセキュリティ確保を図るシステムも採用されている。しかしながら、かかる専用線によるシステムは費用が非常に掛かるため、大規模な企業やオフィスビル、あるいは美術館など、セキュリティ確保に十分な費用を掛けられる一部でのみ採用されているのが現状である。このような背景から、一般の家庭では監視カメラを用いた監視システムを気軽に利用できるまでには至っていない。

【 0 0 0 6 】

また、近年における携帯電話などの携帯端末の普及に伴って発展した新たな監視システムとして、家庭内に設置した監視カメラとユーザが外出時に携帯する携帯端末とを、家庭内に設置したルータなどを用いて仮想施設網（Virtual Private Network：VPN）構成とするシステムがある。VPNによれば、送信側および受信側のそれぞれに暗号処理機能を持たせることで、専用線を引くのと実質的に同様の効果がある。しかしながら、例えば仕事の合間に一時的に家庭内を確認したい場合や専用のモニタを用いて常時監視したい場合など、携帯端末からではなく、コンピュータから監視カメラを確認したいという要請があるが、オフィス内のLAN（Local Area Network）からでは、VPNに接続することが不可能である。

【 0 0 0 7 】

本発明は、従来の監視システムおよび画像伝送システムが有する上記問題点に鑑みてなされたものであり、本発明の目的は、監視目的の画像やモニタリング画

像など他者に見られたくない画像をネットワーク経由で送出するにあたり、他者に見られることなく、本人のみが安全に、ネットワークを介して画像を見ることが可能な、新規かつ改良された画像伝送システム、撮像装置、撮像装置ユニット、鍵生成装置、およびプログラムを提供することである。

【0 0 0 8】

【課題を解決するための手段】

上記課題を解決するため、本発明の第1の観点によれば、ネットワークを介して画像を伝送する画像伝送システムが提供される。本発明の画像伝送システムは、少なくとも以下の構成要素を含むことを特徴とする。

- ・各々が固有の識別番号を有し、撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する1または2以上の撮像装置
- ・画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置ごとに生成する鍵生成装置
- ・復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体
- ・リムーバブル記録媒体が接続され、復号化キーを用いて暗号化された画像を復号化する復号化機能を有し、ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置
- ・閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバ

【0 0 0 9】

かかる画像伝送システムによれば、撮像装置に、画像の暗号化を行う機能を有するようにしたことで、撮像装置内で画像に暗号処理を施すことができ、セキュリティを高めることができる。そして、撮像装置からの画像をネットワークに送出するにあたり、画像を暗号処理した後、ネットワークに送出するようにした。そして、ネットワークに送出された画像は、本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ、復号化して見ることはできない。かかるシステムの実現のため、撮像装置は、各々が固有の識別番号を有している。このようにして、ネットワーク上では画像が暗号化されているため、本人のみが安全に、ネットワークを介して画像を見ることができる。

【0010】

上記課題を解決するため、本発明の第2の観点によれば、ネットワークを介して画像を伝送する画像伝送システムが提供される。本発明の画像伝送システムは、少なくとも以下の構成要素を含むことを特徴とする。

- ・各々が固有の識別番号を有する1または2以上の撮像装置
- ・撮像装置が撮像した画像を暗号化してネットワークに伝送するとともに、暗号化された画像の復号化するための復号化キーを生成する鍵生成装置
- ・復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体
- ・リムーバブル記録媒体が接続され、復号化キーを用いて暗号化された画像を復号化する復号化機能を有し、ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置
- ・閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバ

【0011】

かかる画像伝送システムによれば、鍵生成装置に、画像の暗号化を行う機能を有するようにしたことで、撮像装置が設置された家庭やオフィス内で画像に暗号処理を施すことができ、セキュリティを高めることができる。そして、撮像装置からの画像をネットワークに送出するにあたり、画像を暗号処理した後、ネットワークに送出するようにした。そして、ネットワークに送出された画像は、本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ、復号化して見ることはできない。かかるシステムの実現のため、撮像装置は、各々が固有の識別番号を有している。このようにして、ネットワーク上では画像が暗号化されているため、本人のみが安全に、ネットワークを介して画像を見ることができる。

【0012】

上記課題を解決するため、本発明の第3の観点によれば、ネットワークを介して画像を伝送する画像伝送システムが提供される。本発明の画像伝送システムは、少なくとも以下の構成要素を含むことを特徴とする。

- ・各々が固有の識別番号を有する1または2以上の撮像装置

- ・ 撮像装置が撮像した画像を暗号化してネットワークに伝送する伝送装置
- ・ 画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置ごとに生成する鍵生成装置
- ・ 復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体
- ・ リムーバブル記録媒体が接続され、復号化キーを用いて暗号化された画像を復号化する復号化機能を有し、ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置
- ・ 閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバ

【0013】

かかる画像伝送システムによれば、撮像装置が撮像した画像を暗号化してネットワークに伝送する伝送装置と、画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置ごとに生成する鍵生成装置を別個のシステム構成要素としている。そして、伝送装置に、画像の暗号化を行う機能を有するようにしたことで、撮像装置が設置された家庭やオフィス内で画像に暗号処理を施すことができ、セキュリティを高めることができる。そして、撮像装置からの画像をネットワークに送出するにあたり、画像を暗号処理した後、ネットワークに送出するようにした。そして、ネットワークに送出された画像は、本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ、復号化して見ることはできない。かかるシステムの実現のため、撮像装置は、各々が固有の識別番号を有している。このようにして、ネットワーク上では画像が暗号化されているため、本人のみが安全に、ネットワークを介して画像を見ることができる。

【0014】

上記課題を解決するため、本発明の第4の観点によれば、ネットワークを介して画像を伝送する画像伝送システムが提供される。本発明の画像伝送システムは、少なくとも以下の構成要素を含むことを特徴とする。

- ・ 各々が固有の識別番号を有し、撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する1または2以上の撮像装置

- ・撮像装置が画像を暗号化するための暗号化キーおよび復号化キーを撮像装置ごとに生成する鍵生成装置
- ・復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体
- ・リムーバブル記録媒体が接続され、復号化キーを用いて暗号化された画像を復号化する復号化機能を有し、ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置

【0015】

かかる画像伝送システムによれば、閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバをシステム構成要素としなくても、上記第1の観点にかかる画像伝送システムと同様の効果を得ることができる。すなわち、認証サーバによる管理を行わなくても、撮像装置に、画像の暗号化を行う機能を有するようにしたことで、撮像装置内で画像に暗号処理を施すことができ、撮像装置単体であっても十分にセキュリティを高めることができる。

【0016】

また、上記課題を解決するため、本発明の第5の観点によれば、ネットワークを介して画像を伝送する画像伝送システムに用いられる撮像装置が提供される。本発明の撮像装置は、少なくとも以下の構成要素を備えたことを特徴とする。

- ・固有の識別番号を記録する記録部
- ・撮像した画像を暗号化する暗号化部
- ・暗号化された画像をネットワークに伝送する通信部

【0017】

かかる撮像装置によれば、画像の暗号化を行う暗号化部を備えるようにしたことで、撮像装置内で画像に暗号処理を施すことができ、セキュリティを高めることができる。そして、撮像装置からの画像をネットワークに送出するにあたり、画像を暗号化部で暗号処理した後、通信部からネットワークに送出するようにした。そして、ネットワークに送出された画像は、本人認証を行った後でなければ、復号化して見るができない。かかるシステムの実現のため、撮像装置は、固有の識別番号を記録部に記録している。このようにして、ネットワーク上では

画像が暗号化されているため、本人のみが安全に、ネットワークを介して画像を見ることができる。

【0018】

本発明の撮像装置において、以下のような応用が可能である。

【0019】

通信部が、画像を暗号化するための暗号化キーを鍵生成装置から受信する受信部を含むようにすれば、撮像装置内に暗号化キーを保持しておく必要がなくなり、記憶部の容量を縮小することができる。また、暗号化キーを保持しないため、セキュリティを高めるのにも有効である。

【0020】

また、本発明の撮像装置は、通信部（インタフェース）がUSBポートを含む、いわゆるUSBカメラであってもよい。USB（Universal Serial Bus）は、シリアル・インタフェース規格であり、機器の接続を自動的に認識するプラグ・アンド・プレイ機能や、接続するコンピュータやルータ装置などの電源を入れたままコネクタの抜き差しができるホット・プラグ機能を備えている。また、コンピュータやルータ装置から機器への電源供給も可能である。また、ほとんどのコンピュータやルータ装置などに接続が可能である。このような点で、通信部（インタフェース）がUSBポートを含む、いわゆるUSBカメラであると、利便性が極めて高い。

【0021】

また、撮像装置は、記録手段にIPアドレスを記録した、いわゆるIPカメラであってもよい。IPカメラであれば、10/100BaseのLAN網（イーサネットポート）に接続するだけで、追加のハードウェアを購入することなくネットワーク600上のどのコンピュータからでもアクセスすることができる。

【0022】

また、上記課題を解決するため、本発明の第6の観点によれば、固有の識別番号を有し、撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する撮像装置と、撮像装置が暗号化した画像を復号化するための復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と、を含む

ことを特徴とする、撮像装置ユニットが提供される。

【0023】

かかる撮像装置ユニットによれば、撮像装置に、画像の暗号化を行う機能を有するようにしたことで、撮像装置内で画像に暗号処理を施すことができ、セキュリティを高めることができる。そして、撮像装置からの画像をネットワークに送出するにあたり、画像を暗号処理した後、ネットワークに送出するようにした。そして、ネットワークに送出された画像は、本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ、復号化して見ることはできない。かかるシステムの実現のため、撮像装置は、各々が固有の識別番号を有している。このようにして、ネットワーク上では画像が暗号化されているため、本人のみが安全に、ネットワークを介して画像を見ることができる。

【0024】

本発明の撮像装置ユニットにおいて、以下のような応用が可能である。

【0025】

撮像装置が、画像を暗号化するための暗号化キーを鍵生成装置から受信するようにすれば、撮像装置内に暗号化キーを保持しておく必要がなくなり、記憶部の容量を縮小することができる。また、暗号化キーを保持しないため、セキュリティを高めるのにも有効である。

【0026】

また、リムーバブル記録媒体についても、画像を復号化するための復号化キーを鍵生成装置から受信するようにしてもよい。この場合、暗号化キーを生成する鍵生成装置と復号化キーを生成する鍵生成装置が、同じ鍵生成装置であってもよく、異なる鍵生成装置であってもよい。

【0027】

また、撮像装置は、上記本発明の第5の観点と同様に、USBカメラとしたり、IPカメラとしたりすることができる。

【0028】

また、本発明の第7の観点によれば、ネットワークを介して画像を伝送する際の暗号処理に用いられる暗号化キーおよび復号化キーを生成する鍵生成装置が提

供される。本発明の鍵生成装置は、固有の識別番号を有し、撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する撮像装置に対して、画像を暗号化するための暗号化キーを生成して送出するとともに、暗号化された画像を復号化するための復号化キーを生成して、復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体に送出することを特徴とする。

【 0 0 2 9 】

かかる鍵生成装置によれば、撮像装置が、撮像装置内に暗号化キーを保持しておく必要がなくなり、撮像装置の記憶部の容量を縮小することができる。また、撮像装置が暗号化キーを保持しないため、セキュリティを高めるのにも有効である。

【 0 0 3 0 】

本発明の撮像装置ユニットにおいて、以下のような応用が可能である。

【 0 0 3 1 】

撮像装置をネットワークに中継する中継機能を有するものとすることが可能である。いわゆるルータ装置を鍵生成装置として機能させることができる。

【 0 0 3 2 】

また、撮像装置が撮像した画像を圧縮する圧縮機能を有することも可能である。ネットワークに送出する画像のサイズを縮小化することにより、処理速度を向上させることができる。また、撮像装置に必ずしも圧縮機能を搭載する必要がなくなるため、撮像装置の小型化・低価格化を図ることができる。

【 0 0 3 3 】

また、本発明の第 8 の観点によれば、コンピュータを、上記第 7 の観点にかかる鍵生成装置として機能させるためのプログラムが提供される。ここで、プログラムはいかなるプログラム言語により記述されていてもよい。また、そのプログラムを記録した、コンピュータにより読み取り可能な記録媒体としては、例えば、CD-ROM、DVD-ROM、フロッピーディスク（FD：Floppy Disk）など、プログラムを記録可能な記録媒体として現在一般に用いられている記録媒体、あるいは将来用いられるいかなる記録媒体をも採用することができる。

【0034】**【発明の実施の形態】**

以下に添付図面を参照しながら、本発明にかかる画像伝送システム、撮像装置、撮像装置ユニット、鍵生成装置、およびプログラムの好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

【0035】**(第1の実施の形態)**

図1は、本実施の形態にかかる画像伝送システム10のシステム構成の概略を示す説明図である。なお、図1において括弧書きで示した参照符号は、後述の第2の実施の形態において説明する。本実施の形態にかかる画像伝送システム10について、図1を参照しながら説明する。

【0036】

画像伝送システム10は、図1に示したように、撮像装置100と、鍵生成装置200と、メモリーカード300と、閲覧装置400と、認証サーバ500を含んで構成され、ネットワーク600を介して画像を送送するシステムである。

【0037】

なお、図1において、ネットワーク600は、多数の情報ネットワークを相互に接続することによって世界中に広がったネットワーク環境、例えば、公衆回線網を利用したインターネットを想定している。また、図1には、説明の便宜上、各構成要素を1つずつ示しているが、撮像装置100および鍵生成装置200に相当する構成要素は、一般家庭やオフィスなどに1つまたは2つ以上設置されるものであり、ネットワーク600に極めて多数（例えば、数十万台の規模で）接続されるものである。また、リムーバブル記憶媒体300に相当する構成要素は、撮像装置100と実質的に同数程度存在するものである。また、閲覧装置400に相当する構成要素は、ネットワーク600に接続される任意のコンピュータや携帯電話などであり、ネットワーク600に極めて多数（例えば、数千万台の規模で）接続されるものである。また、認証サーバ500に相当する構成要素は

ネットワーク 600 に複数接続されていてもよい。

【0038】

また、本実施の形態において「画像」とは、撮像装置 100 が撮像対象を光学あるいは音声的に捉え、デジタル化することにより得られたデジタルデータをいい、撮像装置 100 がネットワーク 600 を介して伝送可能な AV (Audio-Video) 情報である。撮像装置 100 の機能に応じて、動画(映像)、静止画(画像)、音声、文字情報など、あるいはこれらの任意の組み合わせをいうものとする。また、撮像装置 100 が画像を得ることを「撮像」という。

【0039】

以下に、本実施の形態にかかる画像伝送システム 10 の各構成要素について詳細に説明する。

【0040】

(撮像装置 100)

撮像装置 100 は、今後家庭やオフィス内に広く普及されると予測される、防犯やペットの監視などに用いられるセキュリティカメラを想定している。すなわち、セキュリティカメラを遠隔地からモニタリングする場合に、画像をネットワーク 600 を介して送出すると、他者からのぞき見られる可能性がある。本実施の形態では、かかるセキュリティカメラの画像を安全にネットワーク上から、どこからでも本人(あるいは本人の承諾を得た者)のみが見られる仕組みについて説明する。

【0041】

本実施の形態では、撮像装置 100 の一例として、USB カメラ 110 と、IP カメラ 120 を例に挙げて説明する。なお、USB カメラ 110 と IP カメラ 120 を区別する必要がないときには、単に撮像装置 100 という。

【0042】

USB カメラ 110 は、コンピュータ用の周辺機器として USB (Universal Serial Bus) 接続可能なカメラである。USB は、シリアル・インタフェース規格であり、機器の接続を自動的に認識するプラグ・アンド・プレイ機能や、接続するコンピュータやルータ装置などの電源を入れたままコ

ネクタの抜き差しができるホット・プラグ機能を備えている。また、コンピュータやルータ装置から機器への電源供給も可能である。そして、ほとんどのコンピュータやルータ装置などに接続が可能である。

【0043】

また、IPカメラ120は、IP (Internet Protocol) を利用したカメラである。IPカメラ120は、IPアドレスを有しており、10/100BaseのLAN網（イーサネットポート）に接続するだけで、追加のハードウェアを購入することなくネットワーク600上のどのコンピュータからでもアクセスすることができる。

【0044】

図2は、IPカメラ120の概略構成を示す説明図である。

IPカメラ120は、図2に示したように、記録部122と、暗号化部124と、インタフェース126と、画像処理部128を備えている。

【0045】

記録部122は、少なくともこのIPカメラ120の固有の識別番号130を記録している。また記録部122は、IPカメラとして機能させるためのIPアドレス132を記録している。さらに記録部122は、後述の鍵生成装置200から伝送され、受信部138で受信した暗号化キー134を記録する。記録部122は、これら識別番号130、IPアドレス132、および暗号化キー134を必要に応じて書き換え（更新）可能なように、例えば、電氣的に内容を書き換えることができるROM (Read Only Memory) であるフラッシュメモリーで構成することができる。

【0046】

暗号化部124は、このIPカメラ120が撮像し、画像処理部128で所定の処理が行われた画像を暗号化する。画像の暗号化には、記録部122に記録された暗号化キー134が用いられる。暗号化方式としては、良く知られた秘密鍵方式（共通鍵方式とも称される）や公開鍵方式などがあるが、本実施の形態では、暗号化キーと復号化キーを同一のキーとする秘密鍵方式を採用することができる。暗号処理を行うための暗号化キーは、後述の鍵生成装置200から送信され

る。

【0047】

インタフェース126は、主に暗号化された画像をネットワーク600に伝送する送信部136と、鍵生成装置200から伝送される暗号化キー134を受信する受信部138とからなる。なお、送信部136と受信部138は、共通のポートであってもよい。また、送信部136または受信部138の規格はどのようなものであってもよい。例えば、受信部138は、USBポートであってもよい。

【0048】

本実施の形態にかかる撮像装置100は、上述のように、記録部122と、暗号化部124と、インタフェース126に特徴を有するものである。撮像装置100の不図示および未説明の構成については、どのようなものであってもよい。

【0049】

撮像装置100は、家庭やオフィスなどに1台または2台以上設置される。撮像装置100は、外部からアクセス可能なように、各々が固有の識別番号を有している。例えば、USBカメラ110の識別番号を「#1」、IPカメラ120の識別番号を「#2」などのように、固有の識別番号がシリアルにあるいはランダムに割り振られている。

【0050】

(鍵生成装置200)

再び図1を参照しながら説明すると、鍵生成装置200は、上述の撮像装置100をネットワーク600に接続する機能を有するとともに、撮像装置100が暗号処理を行うための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置100ごとに生成する装置である。また、本実施の形態では、鍵生成装置200は、撮像装置100からの画像をネットワーク600に伝送するための伝送装置としても機能する。

【0051】

本実施の形態では、鍵生成装置200の一例として、コンピュータ210と、ルータ220を例に挙げて説明する。なお、コンピュータ210とルータ220

を区別する必要がないときには、単に鍵生成装置 200 という。

【0052】

コンピュータ 210 は、デスクトップ型のものでもノート型（ラップトップ型）のものでもよく、あるいはパーム型の PDA（Personal Digital Assistant）と称されるものであってもよい。上述の USB カメラ 110 はコンピュータ 210 の USB 端子に接続可能である。

【0053】

コンピュータ 210 は、撮像装置 100 が暗号処理を行うための暗号化キーおよび暗号化された画像を復号化するための復号化キーを生成する機能を有する。かかる機能の実現のため、例えば、コンピュータ 210 には暗号化キーおよび復号化キーを生成するためのアプリケーションソフトが組み込まれる。かかるアプリケーションソフトは、暗号化キーおよび復号化キーを生成するためのコンピュータプログラムを記録した記録媒体から読み込まれる。

【0054】

ルータ 220 は、LAN 同士や LAN と WAN（Wide Area Network）を相互に接続するための装置である。ルータ 220 は、OSI 基本参照モデルのネットワーク層で、パケット中継処理をする。TCP/IP ネットワークでは、IP アドレス（IP: Internet Protocol）を見て中継経路の制御を行う。データ・リンク層では隣接ノード間もしくは同一セグメント上でしかデータの伝達ができないが、ルータ 200 はデータ・リンク層でのデータ転送機能を組み合わせて、ネットワーク 600 上のあらゆるノード間同士でデータを転送する。上述の IP カメラ 120 はルータ 220 のイーサネットポートに接続可能である。

【0055】

ルータ 220 は、撮像装置 100 が暗号処理を行うための暗号化キーおよび暗号化された画像を復号化するための復号化キーを生成する機能を有する。かかる機能は、ルータ 220 にハードウェア的に組み込まれていてもよい。あるいは、かかる機能の実現のため、例えば、ルータ 220 には暗号化キーおよび復号化キーを生成するためのアプリケーションソフトが組み込まれる。かかるアプリケー

ションソフトは、暗号化キーおよび復号化キーを生成するためのコンピュータプログラムを記録した記録媒体から読み込まれる。

【0056】

鍵生成装置 2 0 0 は、暗号化キーを撮像装置 1 0 0 に送信するとともに、復号化キーを撮像装置 1 0 0 の識別番号と関連付けて、後述のメモリーカード 3 0 0 に記録する。このための手段として、鍵生成装置 2 0 0 は、少なくとも、暗号化キーおよび復号化キーを撮像装置 1 0 0 あるいはメモリーカード 3 0 0 に送信するための送信手段を有している。復号化キーをメモリーカード 3 0 0 に送信するための送信手段の一例として、例えば、メモリーカード 3 0 0 用のカードスロットを設けることも可能である。

【0057】

また、鍵生成装置 2 0 0 には、撮像装置 1 0 0 の識別番号が登録される。このための手段として、鍵生成装置 2 0 0 は、少なくとも、撮像装置 1 0 0 の識別番号の登録を受けるための受信手段と、撮像装置 1 0 0 の識別番号を保持するための記憶手段とを有している。鍵生成装置 2 0 0 は、撮像装置 1 0 0 から送信された識別番号を、ネットワーク 6 0 0 を介して後述の認証サーバ 5 0 0 に送信する。

【0058】

また、鍵生成装置 2 0 0 は、画像圧縮機能を有するようにしてもよい。鍵生成装置 2 0 0 には、通常の M P E G 4 のエンコーダに搭載されるようなマイクロプロセッサ (D i g i t a l S i g n a l P r o c e s s o r : D S P) を搭載することができる。すなわち、撮像装置 1 0 0 が撮像した画像は、鍵生成装置 2 0 0 を介してネットワーク 6 0 0 に送出される。この際、鍵生成装置 2 0 0 は、撮像装置 1 0 0 が圧縮した画像を圧縮した後、ネットワーク 6 0 0 に送出する。これは、後述するように、画像を閲覧するための閲覧装置 4 0 0 について、比較的処理能力の小さい携帯電話なども想定しており、データ量の大きな画像を処理するのが難しい場合を想定したものである。

【0059】

あるいは、鍵生成装置 2 0 0 はネットワーク 6 0 0 に対し、例えば、まず静止

画を送出し、その後に動画（映像）を送出するようにしてもよい。データ量の小さな静止画をいち早く送出的ること、撮像装置 1 0 0 が撮像した情報をユーザにいち早く知らせることができる。例えばユーザ宅への侵入者が撮像装置 1 0 0 や鍵生成装置 2 0 0 が設置されているのに気付いてこれらを壊そうとした場合でも、静止画であれば瞬時に送出的ることができるので、防犯に役立つという利点もある。

【0 0 6 0】

（メモリーカード 3 0 0）

リムーバブル記憶媒体の一例たるメモリーカード 3 0 0 は、ユーザが後述の閲覧装置 4 0 0 を用いて、撮像装置 1 0 0 から伝送される画像を閲覧するために用いられるものである。すなわち、ユーザが閲覧装置 4 0 0 を用いて撮像装置 1 0 0 から伝送させる画像を閲覧する際、メモリーカード 3 0 0 を閲覧装置 4 0 0 に接続し、メモリーカード 3 0 0 に記録された認証情報を用いてユーザ認証を行う。このようにして、撮像装置 1 0 0 から伝送される画像を、認証された本人のみが閲覧することができる。以下に、メモリーカード 3 0 0 について説明する。

【0 0 6 1】

メモリーカード 3 0 0 は、鍵生成装置 2 0 0 が生成した復号化キーと、撮像装置 1 0 0 の識別番号とを関連付けて記録する。1つのメモリーカード 3 0 0 に、1つの撮像装置 1 0 0 を対応付けてもよく、複数の撮像装置 1 0 0 を対応付けてもよい。より具体的には、メモリーカード 3 0 0 には、撮像装置 1 0 0 の識別番号が1つまたは複数予め与えられており、復号化キーは後段階で与えることができる。また、メモリーカード 3 0 0 には、このメモリーカード 3 0 0 を使用するためのパスワードが設定されている。このような各種情報の保持および更新のために、メモリーカード 3 0 0 は、記録内容を書き換え可能な手段で構成することができる。メモリーカード 3 0 0 は、例えば、電氣的に内容を書き換えることができる ROM（Read Only Memory）であるフラッシュメモリーで構成することができる。

【0 0 6 2】

また、メモリーカード 3 0 0 は、上述の鍵生成装置 2 0 0 に接続して復号化キ

ーを受信するための接続手段、および、後述の閲覧装置 400 に接続するための接続手段を有している。これら接続手段は同じものであってもよく、別個のものであってもよい。接続手段としては、例えば、ほとんどのコンピュータやルータ装置などに接続が可能のように、USBコネクタで構成することができる。あるいは、上述の鍵生成装置あるいは後述の閲覧装置 400 の側に、メモリーカード 300 を読み書き可能な手段、例えば、カードスロットなどを設けるようにしてもよい。

【0063】

以上説明したメモリーカード 300 は、上述の撮像装置 100 の付属的構成要素（オプション）として位置づけることができる。メモリーカード 300 は、例えば、撮像装置 100 と一緒に、撮像装置ユニットとして商取引の対象とすることが可能である。メモリーカード 300 は、携帯に便利のように、例えばキーホルダー型、バッジ型、ペン型など様々な形状とすることができる。また、メモリーカード 300 を他の所持品に固着可能なように、例えば磁石や吸盤などを備えることも可能である。

【0064】

また、撮像装置 100 およびメモリーカード 300 を商取引の対象とするにあたり、撮像装置 100 およびメモリーカード 300 を一体にして、撮像装置ユニットとして商取引の対象としてもよい。あるいは、撮像装置 100 のみをまず商取引の対象とし、メモリーカード 300 は事後的にオプションとして商取引の対象としてもよい。

【0065】

（閲覧装置 400）

閲覧装置 400 は、ユーザが、撮像装置 100 から伝送される画像を閲覧するために用いられるものである。すなわち、ユーザが撮像装置 100 から伝送される画像を閲覧する際、上述のメモリーカード 300 を閲覧装置 400 に接続して、ユーザ認証を行う。そして、ユーザ認証を行った後、撮像装置 100 から伝送される画像を閲覧することができる。以下に、閲覧装置 400 について詳細に説明する。

【0066】

本実施の形態では、閲覧装置400の一例として、コンピュータ410と、携帯電話420を例に挙げて説明する。なお、コンピュータ410と携帯電話420を区別する必要がないときには、単に閲覧装置400という。

【0067】

コンピュータ410は、デスクトップ型のものでもノート型（ラップトップ型）のものでもよく、あるいはパーム型のPDA（Personal Digital Assistant）と称されるものであってもよい。コンピュータ410には、ネットワーク600に接続してHTTP（HyperText Transfer Protocol）ファイルを閲覧するためのソフト（ブラウザソフト）が組み込まれている。そして、ブラウザソフトには、撮像装置100からの画像を閲覧するためのプラグインソフトが追加されている。このプラグインソフトによって、画像を閲覧するユーザがパスワードを入力するなどの各種操作を行うことができる。

【0068】

コンピュータ410には、上述のメモリーカード300の記録内容を読み出し可能な手段が設けられている。かかる手段としては、例えばメモリーカード300がUSBコネクタを備えている場合には、USBポートとすることができる。また、メモリーカード300がUSBコネクタを備えていない場合に、コンピュータ410に、カードスロットを設けたり、外部接続機器としてカードリーダを接続したりすることが可能である。

【0069】

携帯電話420は、少なくともネットワーク600を介して画像の受信を行うことができる受信機能と、画像を表示可能な表示機能と、表示部に対する所定の操作を行うための操作部を備えている。その他の機能、例えば音声通話機能や音声や画像の記録機能などについてはどのようなものであってもよい。携帯電話420にも、上述のコンピュータ410に組み込まれるようなプラグインソフトが組み込まれており、画像を閲覧するユーザがパスワードを入力するなどの各種操作を行うことができる。

【0070】

携帯電話 420 には、上述のメモリーカード 300 の記録内容を読み出し可能な手段が設けられている。かかる手段としては、例えばメモリーカード 300 が USB コネクタを備えている場合には、USB ポート、あるいはアダプタを介して USB コネクタを接続可能なポートとすることができる。また、メモリーカード 300 が USB コネクタを備えていない場合に、携帯電話 420 にカードスロットを設けることも可能である。

【0071】

(認証サーバ 500)

認証サーバ 500 は、画像伝送システム 10 において、システム内の認証処理を行うサーバである。すなわち、認証サーバ 500 は、ユーザがメモリーカード 300 を用いて閲覧装置 400 において画像を閲覧する際に、ユーザ認証を行い、ユーザがアクセス可能な撮像装置 100 を認証する。

【0072】

また、認証サーバ 500 の他の機能としては、撮像装置 100 がネットワーク 600 に対して送出する画像を保存することも可能である。撮像装置 100 が監視カメラとして利用されている場合に、撮像装置 100 の画像を保存することで、防犯に効果がある。この際、撮像装置 100 からは静止画および動画（映像）を送ることができる。例えば上述のように、撮像装置 100 からはまず静止画が送られてこれを認証サーバ 500 に保存し、次いで、動画が送られて認証サーバ 500 に保存することができる。

【0073】

以上、図 1 を参照しながら、画像伝送システム 10 の構成について説明した。

次いで、図 3～図 4 を参照しながら、画像伝送システム 10 の初期設定・登録時の動作について説明する。図 3 は、初期設定・登録時の動作をシステム構成とともに示す説明図であり、図 4 は、初期設定・登録時の動作を示す流れ図である。

【0074】

①撮像装置 100 および鍵生成装置 200 の接続

まず、撮像装置 100 (USBカメラ 110 あるいは IPカメラ 120) およびメモリーカード 300 を鍵生成装置 200 に接続する (ステップ S101)。USBカメラ 110 の場合には鍵生成装置 200 に USB 接続され、IPカメラ 120 の場合には鍵生成装置 200 に IP 接続される。また、メモリーカード 300 は鍵生成装置 200 に USB 接続される。

【0075】

②撮像装置 100 から鍵生成装置 200 に対する識別番号の送信

次いで、撮像装置 100 が鍵生成装置 200 に対し、識別番号を送信する。鍵生成装置 200 は、撮像装置 100 から識別番号の送信を受けて、撮像装置 100 の識別番号を登録する (ステップ S102)。

【0076】

③鍵生成装置 200 による暗号化キーおよび復号化キーの生成

鍵生成装置 200 は、撮像装置 100 ごとに固有の暗号化キーおよび復号化キーを生成する (ステップ S103)。例えば、鍵生成装置 200 に USBカメラ 110 と IPカメラ 120 が接続されている場合には、USBカメラ 110 と IPカメラ 120 のそれぞれに固有の識別番号を生成する。暗号化方式として秘密鍵方式 (共通鍵方式) を採用する場合には、暗号化キーと復号化キーを同一のものとすることができる。

【0077】

④鍵生成装置 200 による暗号化キーおよび復号化キーの送信

鍵生成装置 200 は、撮像装置 100 に対し、撮像装置 100 ごとに生成された暗号化キーを記録する。撮像装置 100 において、暗号化キーは、主記憶装置内に暗号化されて記録される。さらに、鍵生成装置 200 は、メモリーカード 300 に対し、復号化キーを記録する (ステップ S104)。

【0078】

⑤鍵生成装置 200 による認証サーバ 500 に対する識別番号の送信

さらに本実施の形態では、鍵生成装置 200 は、ネットワーク 600 を介して認証サーバ 500 に対し、撮像装置 100 の識別番号を登録する (ステップ S105)。

【0 0 7 9】

なお、以上説明した初期設定・登録は、撮像装置 1 0 0 およびメモリーカード 3 0 0 の製造時に製造業者（メーカ）が行ったり、あるいは、撮像装置 1 0 0 およびメモリーカード 3 0 0 の販売時に販売業者（小売店など）が行ってもよい。この場合、事後的に、パスワードの変更や暗号化キー・復号化キーの変更を行えるようにすることがセキュリティ上好ましい。

【0 0 8 0】

以上、図 3 ～図 4 を参照しながら、初期設定・登録時の動作について説明した

。次いで、図 5 ～図 6 を参照しながら、画像伝送システム 1 0 における画像の閲覧時の動作について説明する。図 5 は、画像の閲覧時の動作をシステム構成とともに示す説明図であり、図 6 は、画像の閲覧時の動作を示す流れ図である。

【0 0 8 1】**①撮像装置 1 0 0 による撮像**

上述のように、撮像装置 1 0 0 は、家庭やオフィス内に設置されて、防犯やペットの監視などに用いられるセキュリティカメラを想定している。初期設定・登録が行われた撮像装置 1 0 0 は、家庭やオフィス内に設置されて、家庭やオフィス内の画像を撮像する。撮像された画像は、撮像装置 1 0 0 内で暗号化されて、ネットワークに送出される（ステップ S 2 0 1）。

【0 0 8 2】**②閲覧装置 4 0 0 から認証サーバ 5 0 0 に認証要求**

次いで、撮像装置 1 0 0 が撮像した画像をユーザが遠隔地から閲覧する動作について説明する。閲覧を行うユーザは、上述のメモリーカード 3 0 0 を所持している。このユーザは、遠隔地に設置されたコンピュータ 4 1 0 あるいは所持している携帯電話 4 2 0 などの閲覧装置 4 0 0 から、まず認証サーバ 5 0 0 にアクセスする。この際、ユーザ ID やパスワードなどを入力する。閲覧装置 4 0 0 は、認証サーバ 5 0 0 に対し、このユーザの認証要求を行うとともに、ユーザがアクセス可能な撮像装置 1 0 0 の認証要求を行う（ステップ S 2 0 2）。

【0 0 8 3】

③認証サーバ500が撮像装置100を認証

閲覧装置400からの撮像装置100の認証要求を受けて、認証サーバ500は、ユーザの認証を行うとともに、撮像装置100の認証を行う（ステップS203）。このようにして、閲覧装置400から撮像装置100の閲覧の準備が完了する。

【0084】

④閲覧装置400がメモリーカード300を検出

認証サーバ500により撮像装置100が認証されると、ユーザは、メモリーカード300を閲覧装置400に接続する。なお、ユーザおよび撮像装置100の認証よりも前の段階で、メモリーカード300を閲覧装置400に接続してもよい。そして、閲覧装置400は、メモリーカード300を検出する（ステップS204）。

【0085】

⑤閲覧装置400が、メモリーカード300の識別番号と撮像装置100の識別番号との照合

閲覧装置400は、メモリーカード300を検出すると、メモリーカード300に記録された撮像装置100の識別番号と、認証サーバ500により認証され、画像の伝送を受けようとする撮像装置100の識別番号とを照合する（ステップS205）。

【0086】

⑥復号化キーの取得

メモリーカード300に記録された撮像装置100の識別番号と、画像の伝送を受けようとする撮像装置100の識別番号とが一致すると、閲覧装置400は、メモリーカード300から復号化キーを取得する。そして、閲覧装置400は、その復号化キーを用いて、撮像装置100から伝送される暗号化された画像を復号化する（ステップS206）。

【0087】

⑦閲覧装置400での画像の閲覧

以上の一連の工程を経て、ユーザは、閲覧装置400での画像の閲覧が可能と

なる（ステップ S207）。

【0088】

（第1の実施の形態の効果）

以上説明したように、本実施の形態によれば、撮像装置100に、画像の暗号化を行う機能を有するようにしたことで、撮像装置100内で画像に暗号処理を施すことができ、セキュリティを高めることができる。

【0089】

また、撮像装置100からの画像をネットワーク600に送出するにあたり、画像を暗号化部124で暗号処理した後、ネットワーク600に送出するようにした。そして、ネットワーク600に送出された画像は、本人のみが所有するメモリーカード300を用いて本人認証を行った後でなければ、復号化して見ることができない。このようにして、ネットワーク600上では画像が暗号化されているため、本人のみが安全に、ネットワーク600を介して画像を見ることができる。

【0090】

また、閲覧装置400で閲覧するにあたり、暗号化された画像の復号化キーをメモリーカード300に記録し、このメモリーカード300を使用するためのパスワードを設定している。このため、メモリーカード300を盗難あるいは紛失するなどした場合であっても、悪意ある第三者によるメモリーカード300の不正使用を防止することができる。

【0091】

（第2の実施の形態）

上記第1の実施の形態にかかる画像閲覧システム10は、撮像装置100で画像を暗号化するものであった。本実施の形態では、撮像装置100で画像を暗号化する代わりに、鍵生成装置200で画像を暗号化するシステムについて説明する。

【0092】

本実施の形態にかかる画像伝送システム20のシステム構成の概略は、図1に示したものと実質的に同様であるので、重複説明を省略する。なお、図1におい

て、本実施の形態にかかるシステム構成要素を、括弧書き符号で示している。

【0093】

本実施の形態では、撮像装置100は暗号化機能を備えていない。撮像装置101の一例として、図7に示したIPカメラ120'を例に挙げて説明する。なお、上記第1の実施の形態と同様の構成要素については、同一の参照番号を付すことで重複説明を省略する。図7に示した本実施の形態のIPカメラ120は、図2に示したIPカメラ120と対比して、暗号化部124と受信部138に相当する構成要素を必須の構成要素としない。そして、記録部122は、暗号化キー134を記録していない。すなわち、本実施の形態では、撮像装置100において、画像の撮像のみを行い、撮像した画像の暗号化は行わない。

【0094】

本実施の形態では、撮像装置100から鍵生成装置200に対して、暗号化されていない画像が送出される。そして、鍵生成装置200は、撮像装置100から送出された画像を暗号化する。鍵生成装置200の暗号化機能については、上記第1の実施の形態で説明した、撮像装置100の暗号化部124と実質的に同様のものとしてすることができる。

【0095】

次いで、図8～図9を参照しながら、画像伝送システム20の初期設定・登録時の動作について説明する。図8は、初期設定・登録時の動作をシステム構成とともに示す説明図であり、図9は、初期設定・登録時の動作を示す流れ図である。

【0096】

上記第1の実施の形態との相違点についてのみ説明する。

本実施の形態では、鍵生成装置200は、撮像装置100に対して暗号化キーを渡す動作を行わない。すなわち、図8に示したように、図3に示した「④暗号化キー」の動作が行われない。また、図9に示したように、図4に示したステップS104は、鍵生成サーバ200がメモリーカード300に対し復号化キーを記録する（ステップS104'）という動作に置き換わる。この動作以外については、上記第1の実施の形態と実質的に同様である。

【0097】

次いで、図10～図11を参照しながら、画像伝送システム20における画像の閲覧時の動作について説明する。図10は、画像の閲覧時の動作をシステム構成とともに示す説明図であり、図11は、画像の閲覧時の動作を示す流れ図である。

【0098】

上記第1の実施の形態との相違点についてのみ説明する。

図10には、鍵生成装置200を示している。そして、①撮像装置100で撮像された画像は、鍵生成装置200において暗号化される。また、図11に示したように、図6に示したステップS201は、撮像装置100による撮像、鍵生成装置200による画像の暗号化（ステップS201'）という動作に置き換わる。この動作以外については、上記第1の実施の形態と実質的に同様である。

【0099】

（第2の実施の形態の効果）

以上説明したように、本実施の形態によれば、鍵生成装置200に、画像の暗号化を行う機能を有するようにしたことで、上記第1の実施の形態と実質的に同様の効果を得ることが可能である。

【0100】

さらに、撮像装置100内に暗号化部を備える必要がないので、装置規模を縮小することができる。また、撮像装置100内に暗号化キーを保持しておく必要がなくなり、記憶部の容量を縮小することができる。また、撮像装置100内に暗号化キーを保持しないため、セキュリティを高めるのにも有効である。

【0101】

（第3の実施の形態）

上記第2の実施の形態にかかる画像閲覧システム20は、撮像装置100で画像を暗号化する代わりに、鍵生成装置200で画像を暗号化するものであった。そして、第2の実施の形態にかかる鍵生成装置200は、撮像装置100をネットワーク600に接続する手段と、暗号化キーおよび復号化キーを生成する手段とを兼ねたシステム構成要素である。本実施の形態では、撮像装置100をネッ

トワーク 6 0 0 に接続する手段と、暗号化キーおよび復号化キーを生成する手段とを別個の独立した構成要素としたシステムについて説明する。

【0 1 0 2】

図 1 2 は、本実施の形態にかかる画像伝送システム 3 0 のシステム構成の概略を示す説明図である。本実施の形態にかかる画像伝送システム 3 0 について、図 8 を参照しながら説明する。

【0 1 0 3】

画像伝送システム 3 0 は、図 1 2 に示したように、第 2 の実施の形態にかかる画像伝送システム 2 0 と比較して、鍵生成装置 2 0 0 と伝送装置 2 5 0 とを別個の装置して構成したものである。

【0 1 0 4】

本実施の形態にかかる鍵生成装置 2 0 0 は、画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを生成する機能を有する。かかる機能の実現のため、例えば、鍵生成装置 2 0 0 には暗号化キーおよび復号化キーを生成するためのアプリケーションソフトが組み込まれる。かかるアプリケーションソフトは、暗号化キーおよび復号化キーを生成するためのコンピュータプログラムを記録した記録媒体から読み込まれる。

【0 1 0 5】

また、鍵生成装置 2 0 0 は、暗号化キーを撮像装置 1 0 0 に送信するとともに、復号化キーを撮像装置 1 0 0 の識別番号と関連付けて、メモリーカード 3 0 0 に記録する。このための手段として、鍵生成装置 2 0 0 は、少なくとも、暗号化キーおよび復号化キーを撮像装置 1 0 0 あるいはメモリーカード 3 0 0 に送信するための送信手段を有している。復号化キーをメモリーカード 3 0 0 に送信するための送信手段の一例として、例えば、メモリーカード 3 0 0 用のカードスロットを設けることも可能である。

【0 1 0 6】

また、鍵生成装置 2 0 0 には、撮像装置 1 0 0 の識別番号が登録される。このための手段として、鍵生成装置 2 0 0 は、少なくとも、撮像装置 1 0 0 の識別番号の登録を受けるための受信手段と、撮像装置 1 0 0 の識別番号を保持するため

の記憶手段とを有している。鍵生成装置 200 は、撮像装置 100 から送信された識別番号を、ネットワーク 600 を介して認証サーバ 500 に送信する。

【0107】

一方、本実施の形態にかかる伝送装置 250 は、撮像装置 100 が撮像した画像を暗号化して前記ネットワークに伝送する。伝送装置 250 は、画像圧縮機能を有するようにしてもよい。伝送装置 250 には、通常の M P E G 4 のエンコーダに搭載されるようなマイクロプロセッサ (D i g i t a l S i g n a l P r o c e s s o r : D S P) を搭載することができる。

【0108】

画像伝送システム 30 の初期設定・登録時の動作、および、画像の閲覧時の動作については、上記第 2 の実施の形態と実質的に同様であるので、重複説明を省略する。

【0109】

(第 3 の実施の形態の効果)

以上説明したように、本実施の形態によれば、撮像装置 100 が撮像した画像を暗号化してネットワーク 600 に伝送する伝送装置 250 と、画像を暗号化するための暗号化キーおよび前記暗号化された画像を復号化するための復号化キーを撮像装置 100 ごとに生成する鍵生成装置 200 を別個のシステム構成要素とすることで、上記第 2 の実施の形態と実質的に同様の効果を得ることが可能である。

【0110】

(第 4 の実施の形態)

上記第 1 の実施の形態にかかる画像閲覧システム 10 は、システム構成要素として認証サーバ 500 を含むものであった。本実施の形態では、システム構成要素として認証サーバ 500 を含まないシステムについて説明する。

【0111】

図 13 は、本実施の形態にかかる画像伝送システム 20 のシステム構成の概略を示す説明図である。本実施の形態にかかる画像伝送システム 20 について、図 8 を参照しながら説明する。

【0112】

画像伝送システム40は、図13に示したように、第1の実施の形態にかかる画像伝送システム10と比較して、認証サーバ500を含むことなく構成されたシステムである。

【0113】

次いで、図14～図15を参照しながら、画像伝送システム40の初期設定・登録時の動作について説明する。図14は、初期設定・登録時の動作をシステム構成とともに示す説明図であり、図15は、初期設定・登録時の動作を示す流れ図である。

【0114】

上記第1の実施の形態との相違点についてのみ説明する。

本実施の形態では、①撮像装置100および鍵生成装置200の接続動作（ステップS101）、②撮像装置100から鍵生成装置200に対する識別番号の送信、鍵生成装置200による撮像装置100の識別番号の登録動作（ステップS102）、③鍵生成装置200による暗号化キーおよび復号化キーの生成動作（ステップS103）、④鍵生成装置200による暗号化キーおよび復号化キーの送信動作（ステップS104）については、上記第1の実施の形態と実質的に同様である。

【0115】

本実施の形態では、鍵生成装置200は、認証サーバ500に対して撮像装置100の識別番号を登録する動作を行わない。すなわち、鍵生成装置200が、撮像装置100に対し暗号化キーを、メモリーカード300に復号化キーを記録する動作（ステップS104）を以て、初期設定・登録時の動作は終了する。

【0116】

次いで、図16～図17を参照しながら、画像伝送システム40における画像の閲覧時の動作について説明する。図16は、画像の閲覧時の動作をシステム構成とともに示す説明図であり、図17は、画像の閲覧時の動作を示す流れ図である。

【0117】

上記第 1 の実施の形態との相違点についてのみ説明する。

本実施の形態では、認証サーバ 500 をシステム構成要素として含まない。その結果として、閲覧装置 400 による認証サーバ 500 に対する認証要求は行われず、認証サーバ 500 による撮像装置 100 の認証も行われない。すなわち、図 16 に示したように、図 1 に示した「②認証サーバ 500 に対する認証要求」、および、「③認証サーバ 500 による撮像装置 100 の認証」の動作が行われない。また、図 17 に示したように、図 2 に示したステップ S202 およびステップ S203 は行われない。この動作以外については、上記第 1 の実施の形態と実質的に同様である。

【0118】

(第 4 の実施の形態の効果)

以上説明したように、本実施の形態によれば、第 1 の実施の形態にかかる認証サーバ 500 をシステム構成要素としなくても、上記第 1 の実施の形態と実質的に同様の効果を得ることができる。このため、撮像装置 100 とメモリーカード 300 とを組み合わせた撮像装置ユニットがあれば、認証サーバ 500 による管理の必要がなく、上記第 1 の実施の形態と実質的に同様の効果を得ることができる。

【0119】

以上、添付図面を参照しながら本発明にかかる画像伝送システム、撮像装置、撮像装置ユニット、鍵生成装置、およびプログラムの好適な実施形態について説明したが、本発明はかかる例に限定されない。当業者であれば、特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【0120】

例えば、上記実施の形態では、メモリーカード 300 を使用するためのパスワードを設定することで、メモリーカード 300 を盗難あるいは紛失するなどした場合であっても、悪意ある第三者によるメモリーカード 300 の不正使用を防止することができる点について説明した。しかしながら、パスワードを所定期間以

上にわたって固定しておくことは、セキュリティ上好ましくない。そこで、パスワードを定期的書き換え可能なようにしてもよい。例えば、メモリーカード 3 0 0 を閲覧装置 4 0 0 に接続するたびごとに、パスワードの変更を確認するようにしてもよい。

【 0 1 2 1 】

あるいは、メモリーカード 3 0 0 を閲覧装置 4 0 0 に接続するたびごとに、認証サーバ 5 0 0 がワンタイムパスワード（使い捨てパスワード、ダイナミックパスワードとも称される。）を発行し、これを用いて閲覧を行うようにしてもよい。ワンタイムパスワードは、利用者が使うたびにデータが変わるパスワードである。パスワードが第三者に漏れても、固定的なパスワードのように繰り返して使うことができないので、安全性が極めて高い。例えば、上記実施の形態のように、画像伝送システムをホームセキュリティサービスに用いる場合、画像を長時間見続けるということは希である。そこで、1つのワンタイムパスワードで閲覧できる時間を例えば 3 0 分などのように設定しておくことができる。仮にメモリーカード 3 0 0 を紛失等し、悪意ある第三者が入手した場合でも、わずか 1 回 3 0 分の閲覧しかできないので、被害を最小限にすることができる。ワンタイムパスワードは、閲覧装置 4 0 0 で得るようにしてもよく、他の機器、例えば携帯電話やワンタイムパスワードを発行する専用モジュールから得るようにしてもよい。

【 0 1 2 2 】

また、上記第 4 の実施の形態では、第 1 の実施の形態と比較して、システム構成要素として認証サーバ 5 0 0 を含まないシステムについて説明した。第 2 の実施の形態および第 3 の実施の形態についても、同様に、認証サーバ 5 0 0 を含まないシステムとすることも可能である。

【 0 1 2 3 】

【発明の効果】

以上説明したように、本発明によれば、撮像装置に、画像の暗号化を行う機能を有するようにしたことで、撮像装置内で画像に暗号処理を施すことができ、セキュリティを高めることができる。そして、撮像装置からの画像をネットワークに送出するにあたり、画像を暗号処理した後、ネットワークに送出するようにし

た。そして、ネットワークに送出された画像は、本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ、復号化して見ることはできない。かかるシステムの実現のため、撮像装置は、各々が固有の識別番号を有している。このようにして、ネットワーク上では画像が暗号化されているため、本人のみが安全に、ネットワークを介して画像を見ることができる。

【図面の簡単な説明】

【図 1】

第 1 の実施の形態にかかる画像伝送システムの構成の一例を示す説明図である。

【図 2】

第 1 の実施の形態にかかる I P カメラの構成を示す説明図である。

【図 3】

第 1 の実施の形態にかかる初期設定・登録時の動作をシステム構成とともに示す説明図である。

【図 4】

第 1 の実施の形態にかかる初期設定・登録時の動作を示す流れ図である。

【図 5】

第 1 の実施の形態にかかる画像の閲覧時の動作をシステム構成とともに示す説明図である。

【図 6】

第 1 の実施の形態にかかる画像の閲覧時の動作を示す流れ図である。

【図 7】

第 2 の実施の形態にかかる I P カメラの構成を示す説明図である。

【図 8】

第 2 の実施の形態にかかる初期設定・登録時の動作をシステム構成とともに示す説明図である。

【図 9】

第 2 の実施の形態にかかる初期設定・登録時の動作を示す流れ図である。

【図 1 0】

第 2 の実施の形態にかかる画像の閲覧時の動作をシステム構成とともに示す説明図である。

【図 1 1】

第 2 の実施の形態にかかる画像の閲覧時の動作を示す流れ図である。

【図 1 2】

第 3 の実施の形態にかかる画像伝送システムの構成の一例を示す説明図である。

【図 1 3】

第 4 の実施の形態にかかる画像伝送システムの構成の一例を示す説明図である。

【図 1 4】

第 4 の実施の形態にかかる初期設定・登録時の動作をシステム構成とともに示す説明図である。

【図 1 5】

第 4 の実施の形態にかかる初期設定・登録時の動作を示す流れ図である。

【図 1 6】

第 4 の実施の形態にかかる画像の閲覧時の動作をシステム構成とともに示す説明図である。

【図 1 7】

第 4 の実施の形態にかかる画像の閲覧時の動作を示す流れ図である。

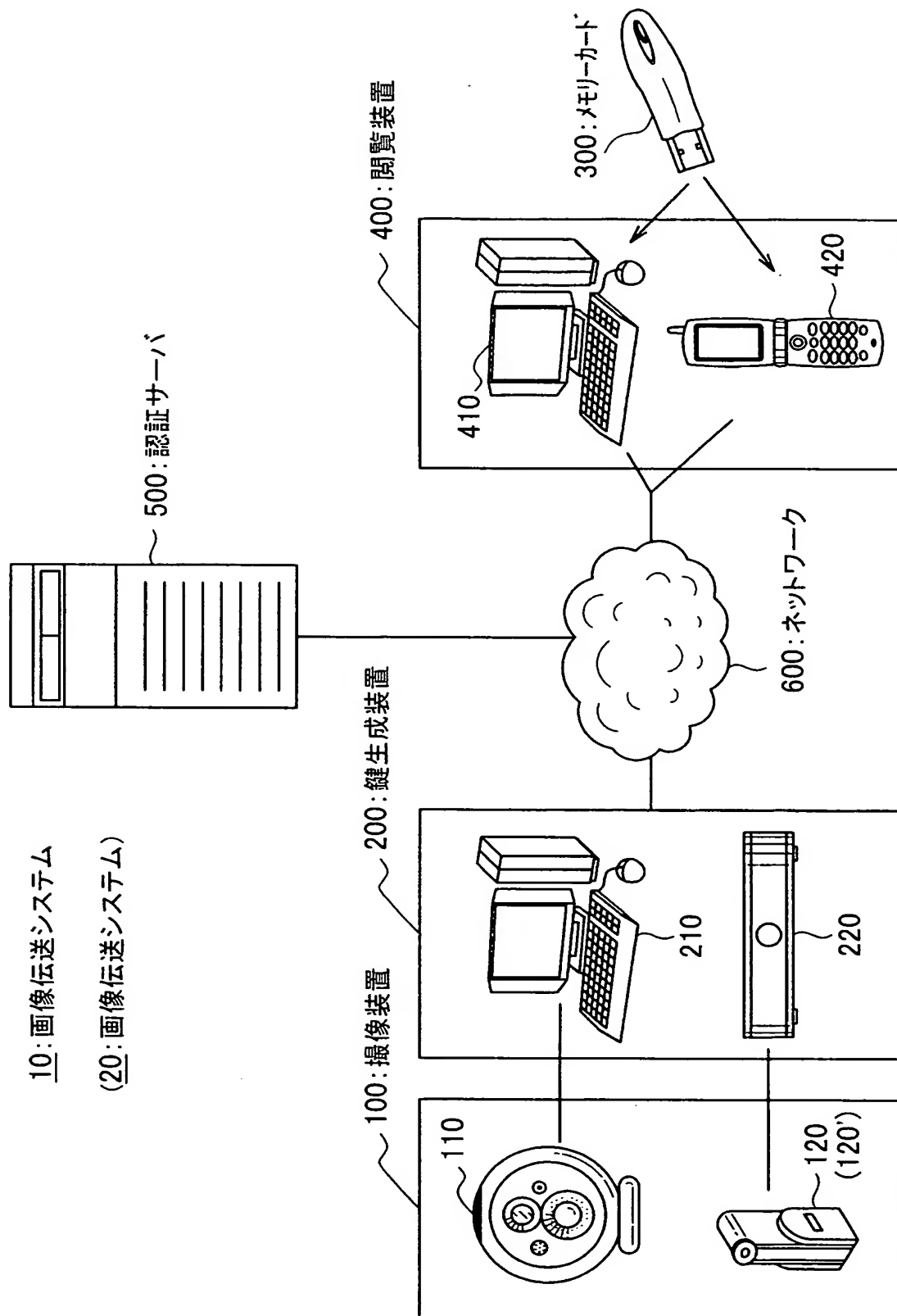
【符号の説明】

- 1 0 画像伝送システム
- 1 0 0 撮像装置
- 1 1 0 U S B カメラ
- 1 2 0 I P カメラ
- 2 0 0 鍵生成装置
- 2 1 0 コンピュータ
- 2 2 0 ルータ
- 3 0 0 メモリーカード（リムーバブル記憶媒体）

- 4 0 0 閲覧装置
- 4 1 0 コンピュータ
- 4 2 0 携帯電話
- 5 0 0 認証サーバ
- 6 0 0 ネットワーク

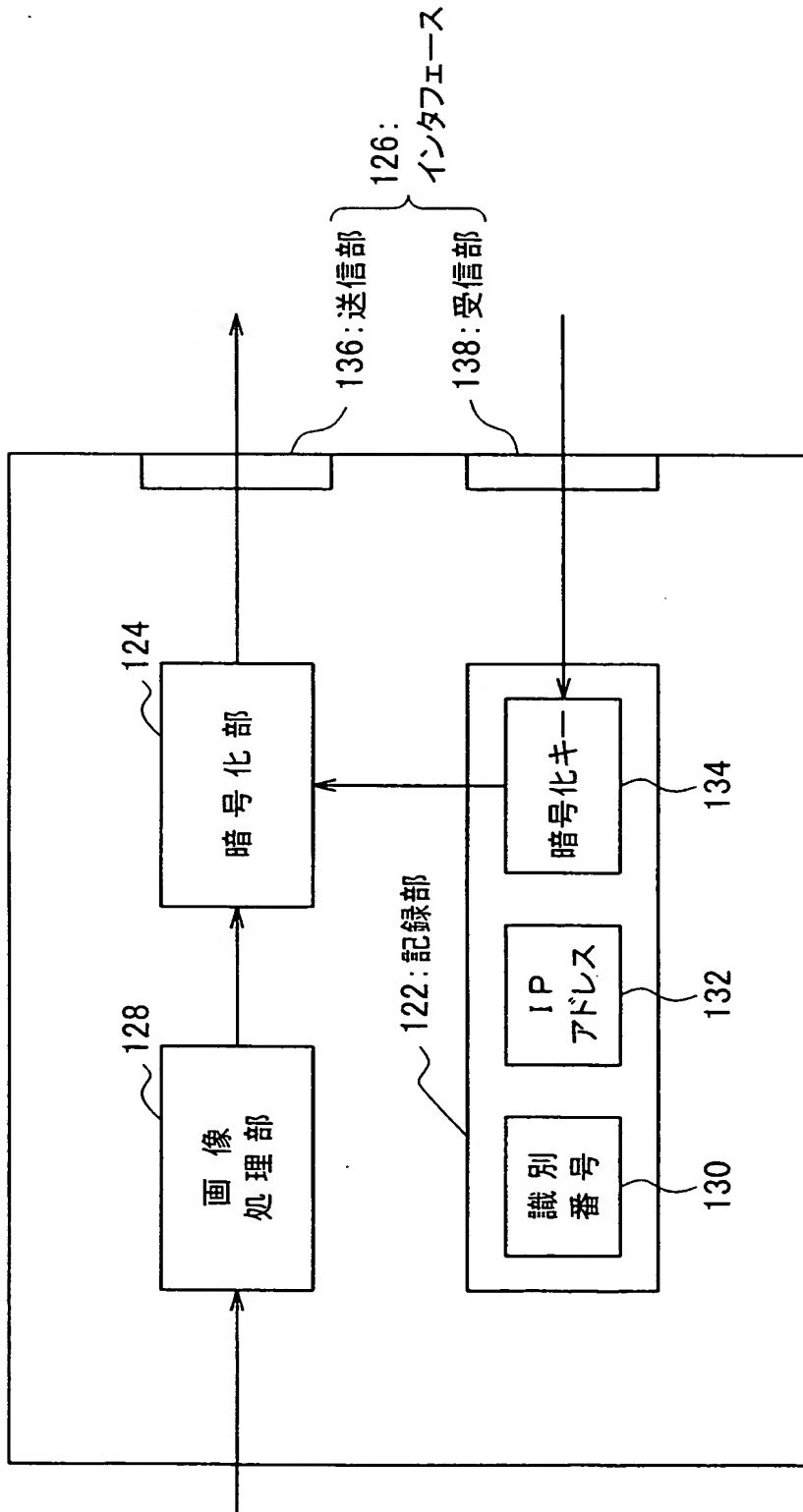
【書類名】 図面

【図 1】

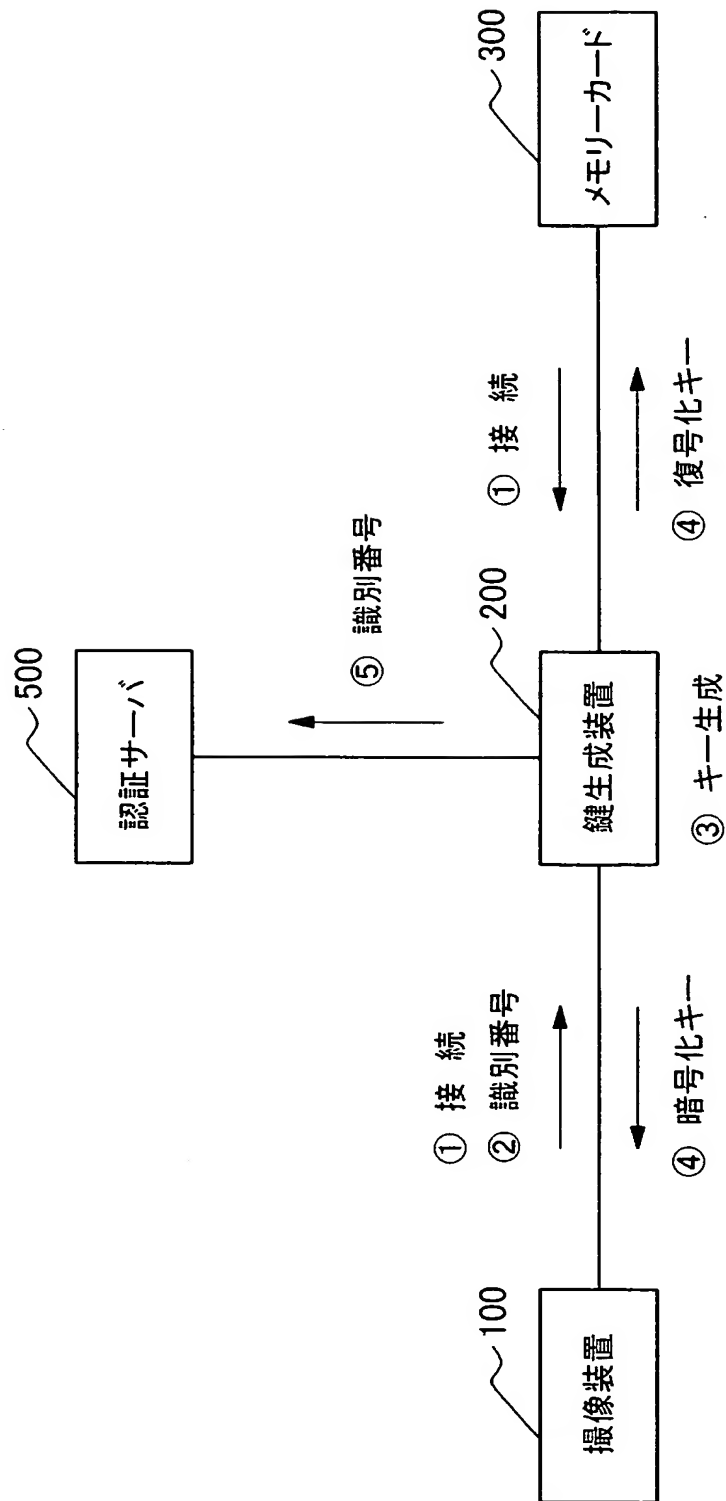


【図 2】

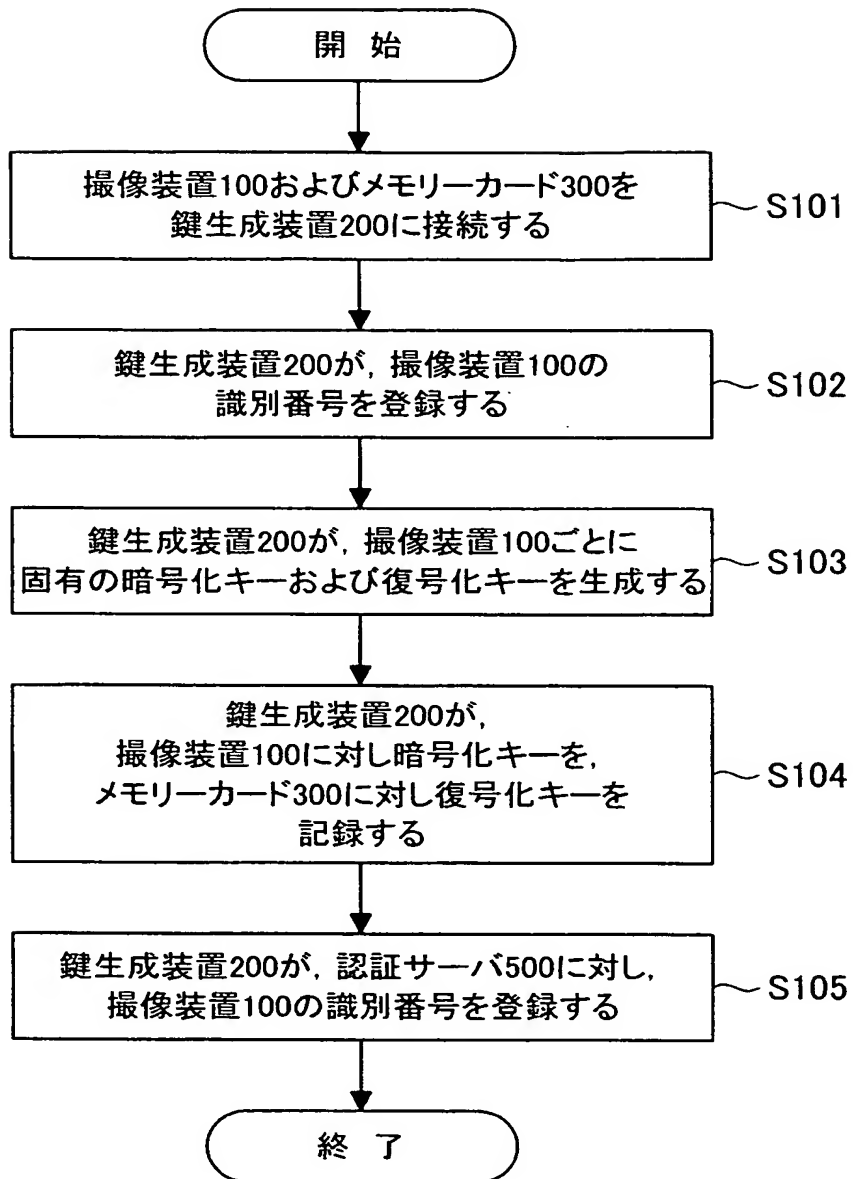
120: IPカメラ



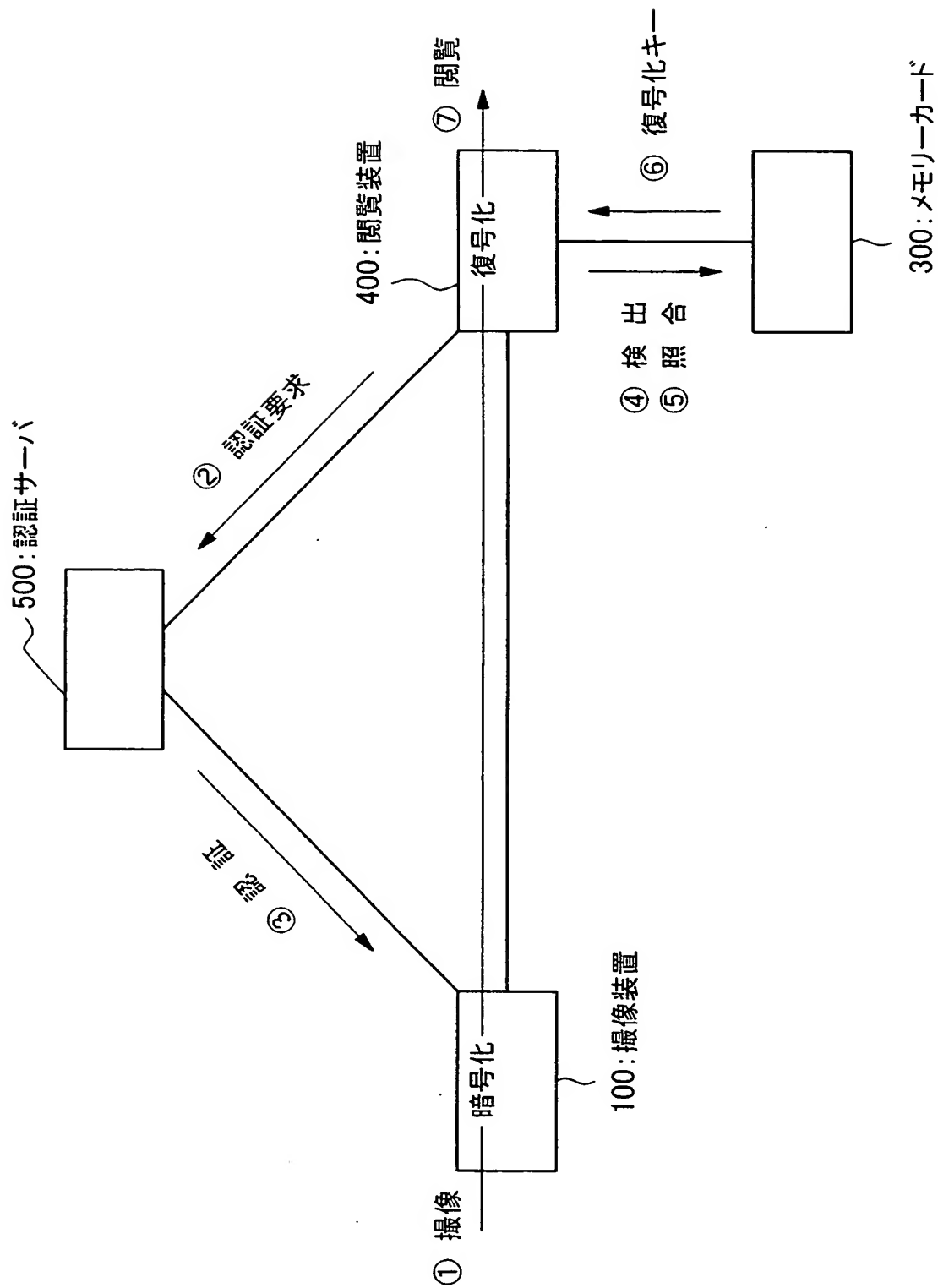
【図 3】



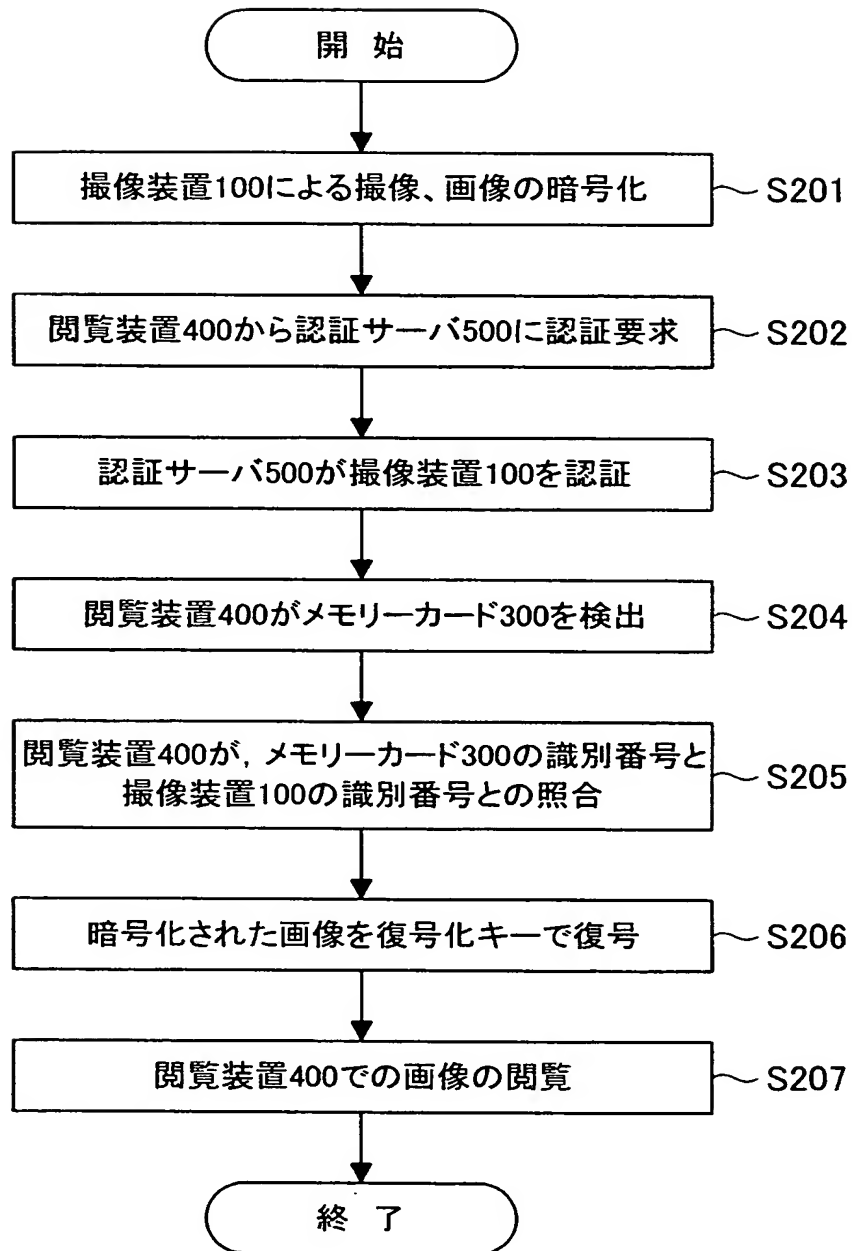
【図 4】



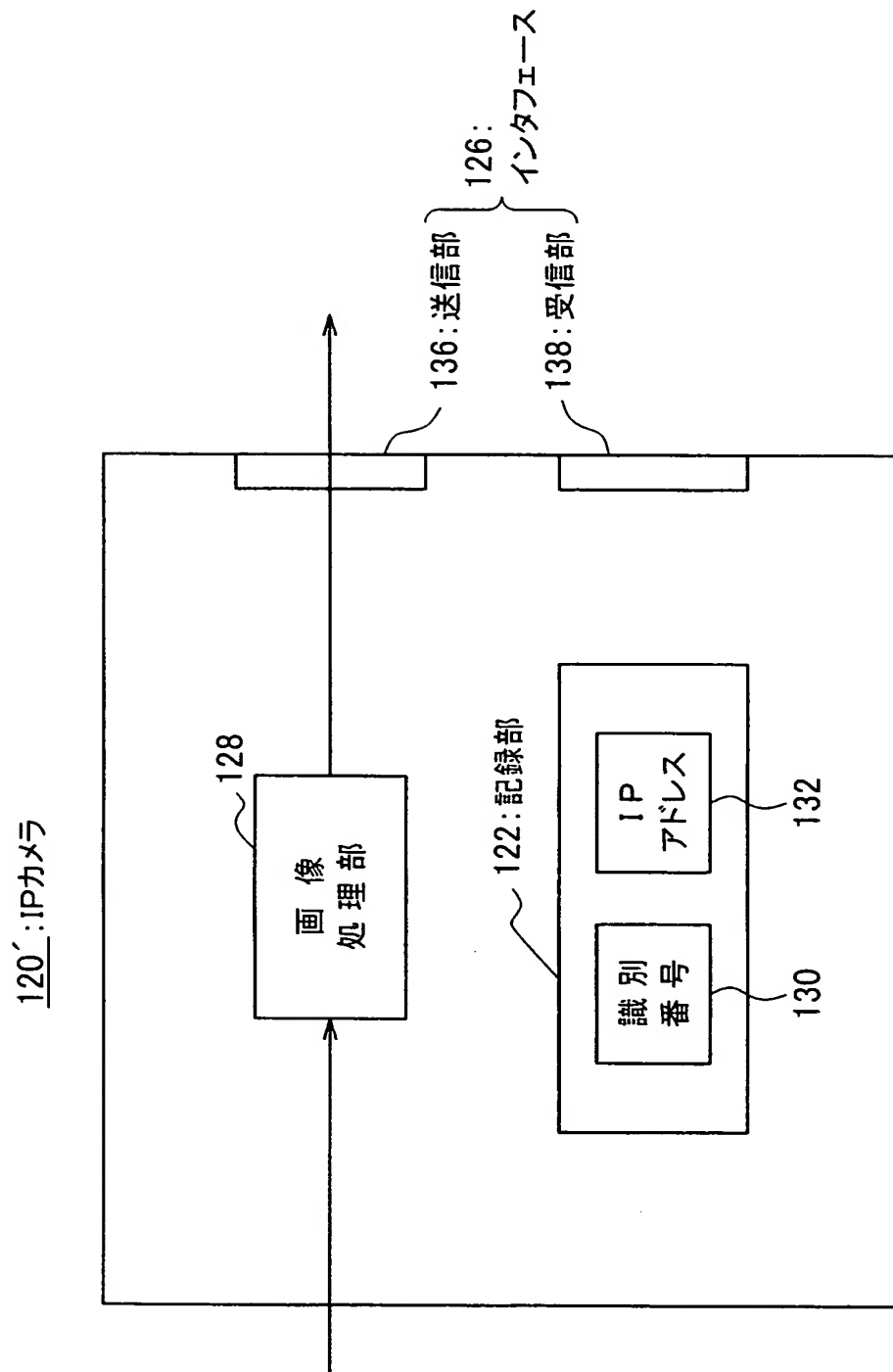
【図 5】



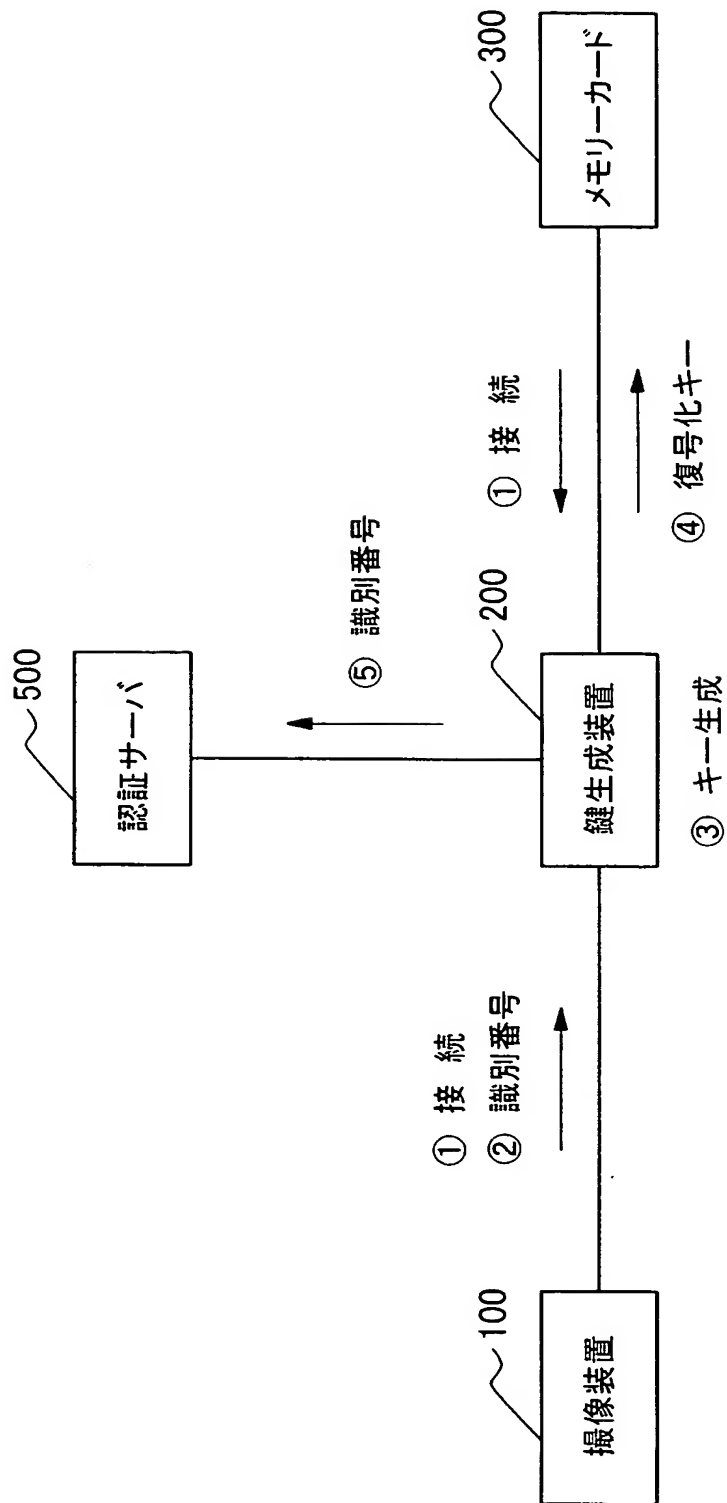
【図 6】



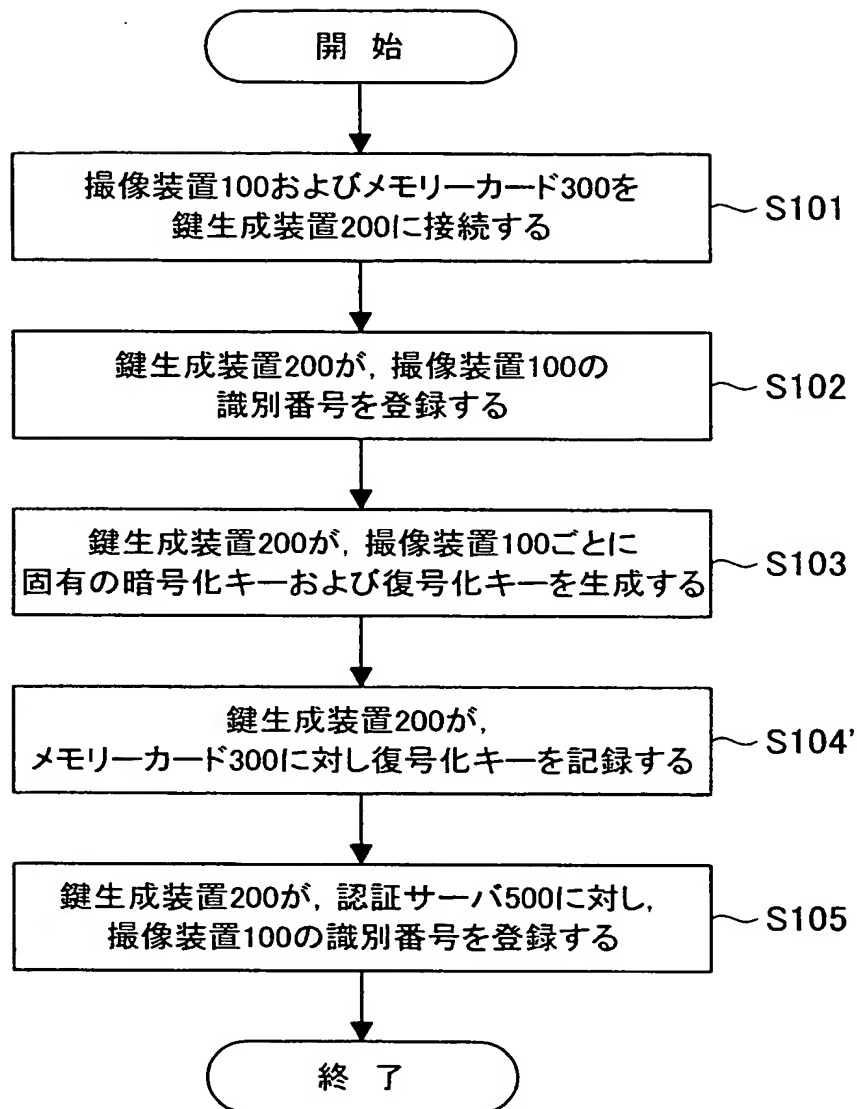
【図 7】



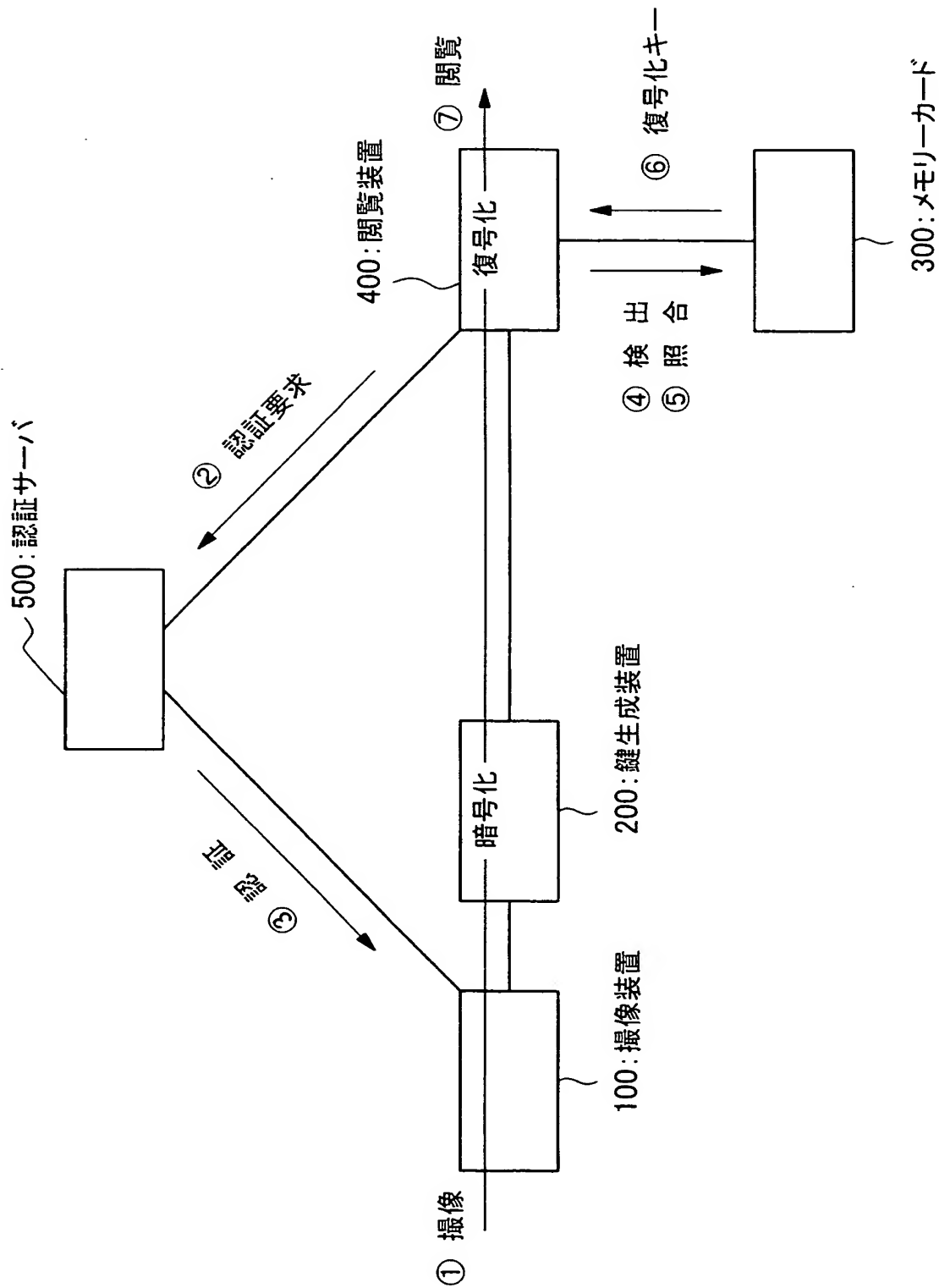
【図 8】



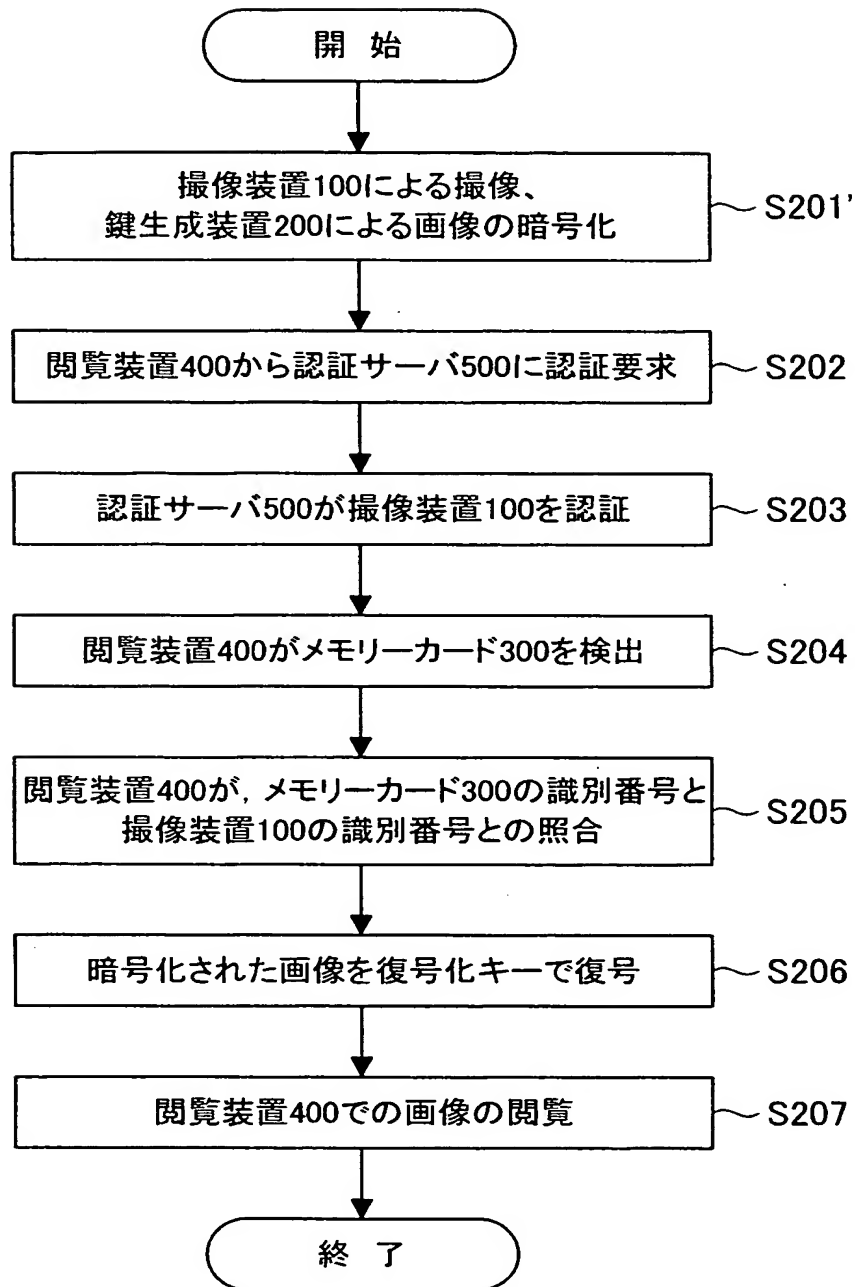
【図 9】



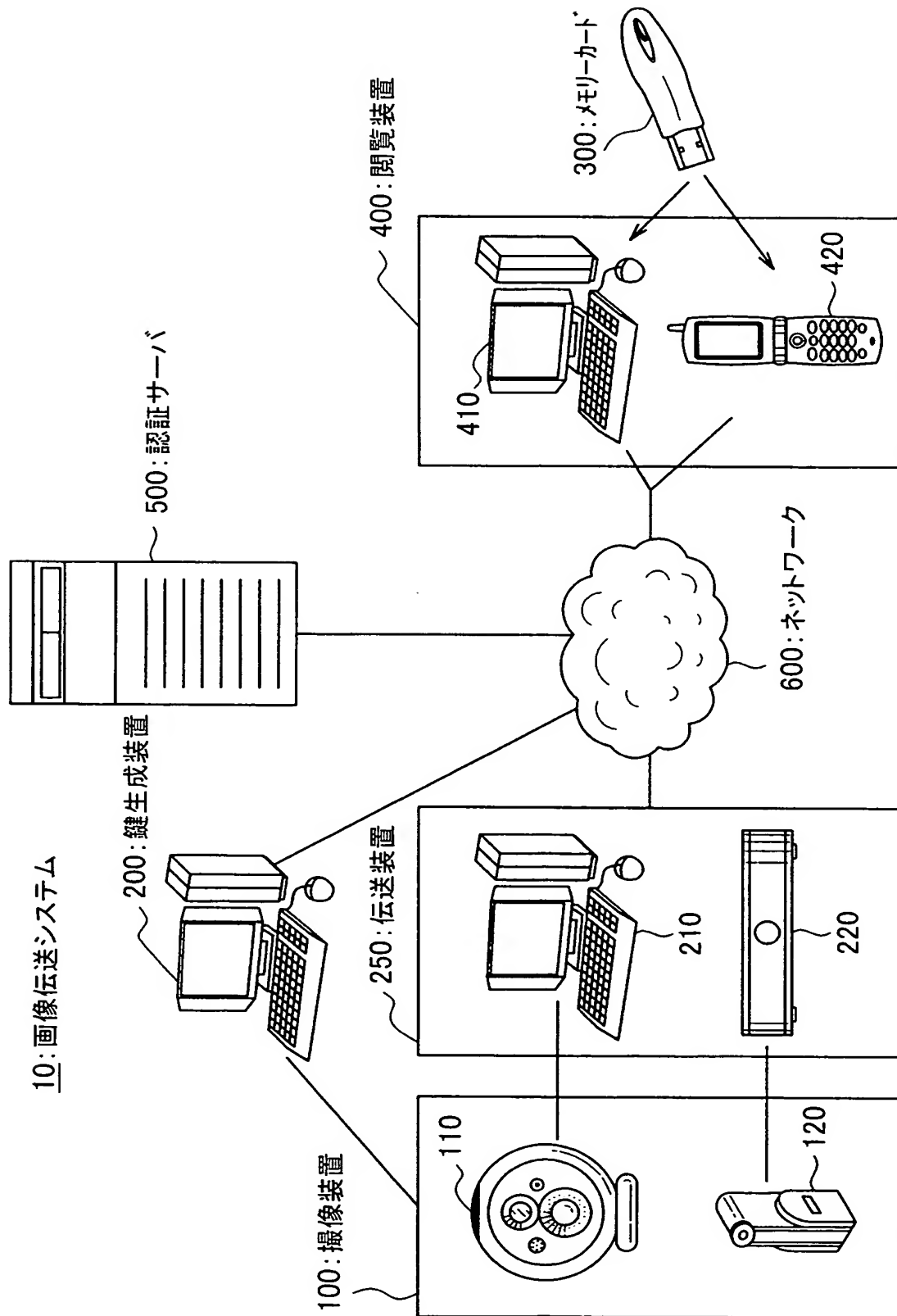
【図 10】



【図 11】

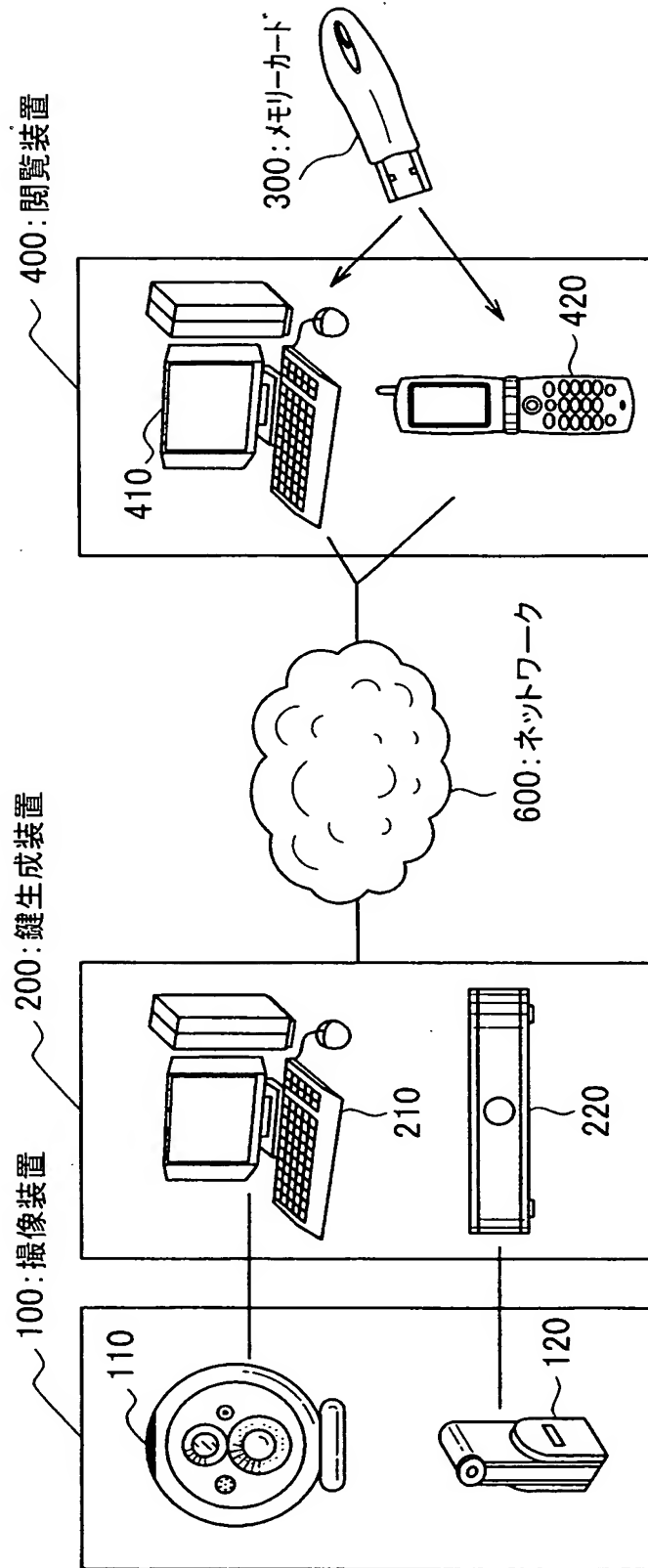


【図 12】

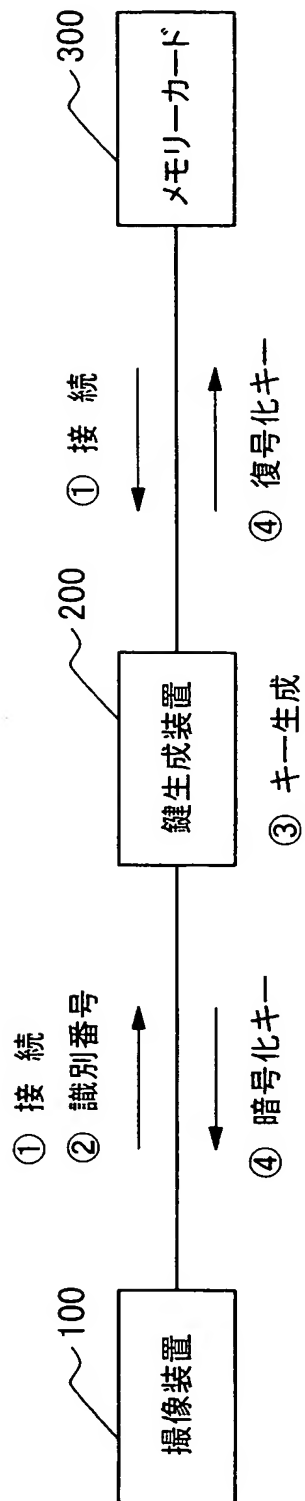


【図 13】

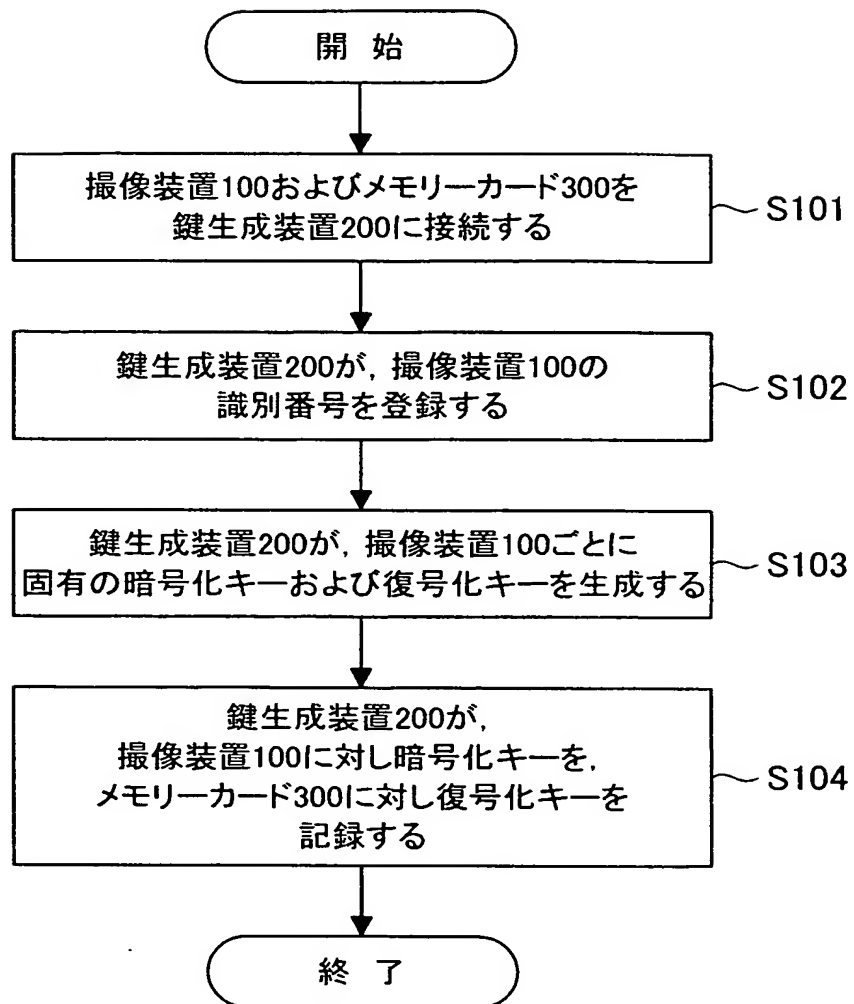
40:画像伝送システム



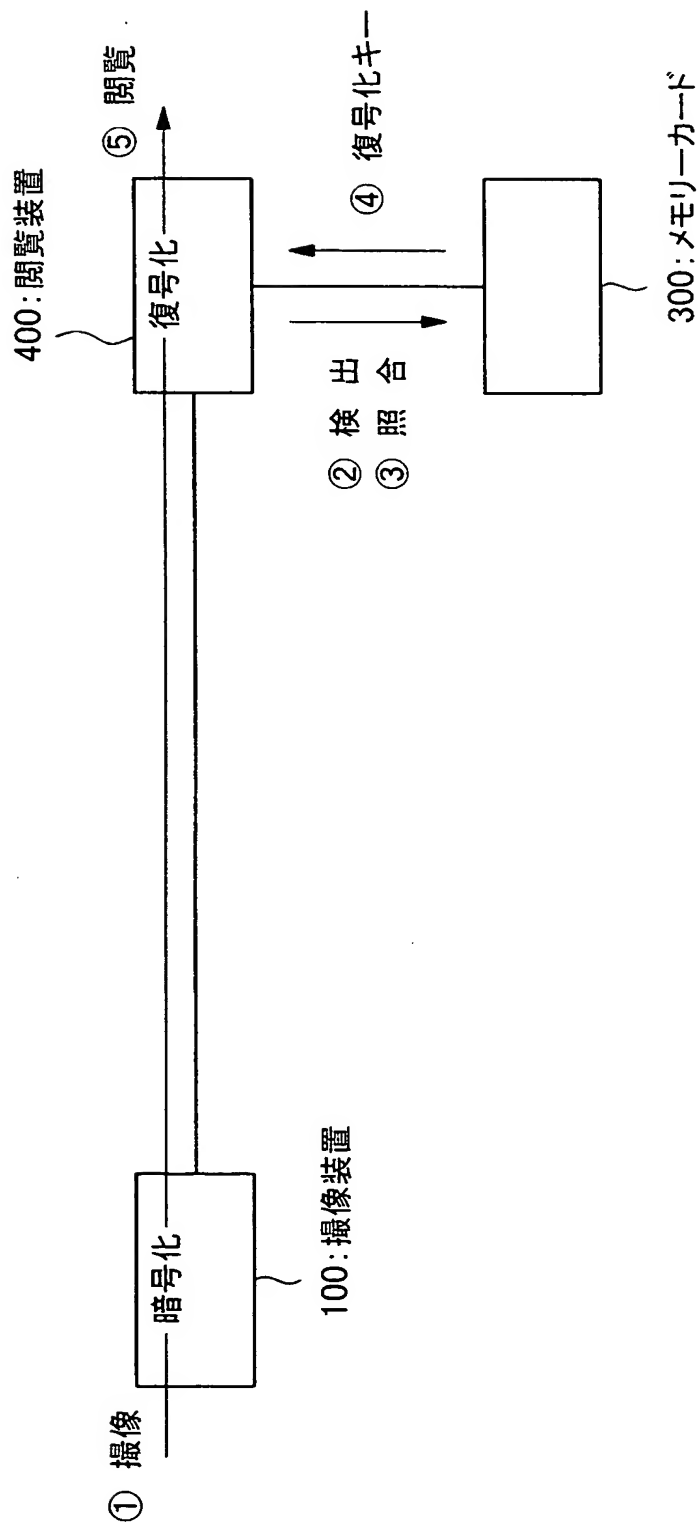
【図 14】



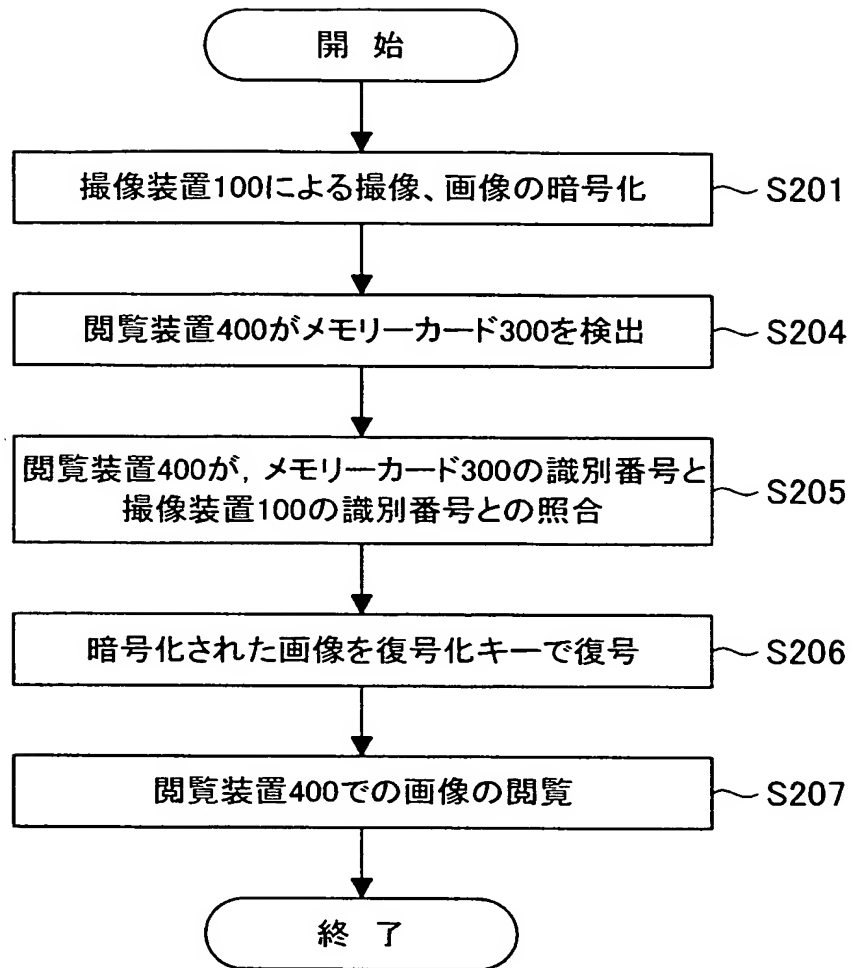
【図 15】



【図 16】



【図 17】



【書類名】 要約書

【要約】

【課題】 他者に見られたくない画像をネットワーク経由で送出するにあたり、本人のみが安全に画像を見ることの可能な、画像伝送システムを提供する。

【解決手段】 画像伝送システム 1 0 は、各々が固有の識別番号を有し、撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する 1 または 2 以上の撮像装置 1 0 0 と、画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置ごとに生成する鍵生成装置 2 0 0 と、復号化キーと撮像装置の識別番号とを関連付けて記録するメモリーカード 3 0 0 と、メモリーカードが接続され、復号化キーを用いて暗号化された画像を復号化する復号化機能を有し、ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置 4 0 0 と、閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバ 5 0 0 を含む。

【選択図】 図 1

特願 2 0 0 3 - 1 0 1 7 8 3

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 2 1 8 5]

1. 変更年月日	1 9 9 0 年 8 月 3 0 日
[変更理由]	新規登録
住 所	東京都品川区北品川 6 丁目 7 番 3 5 号
氏 名	ソニー株式会社